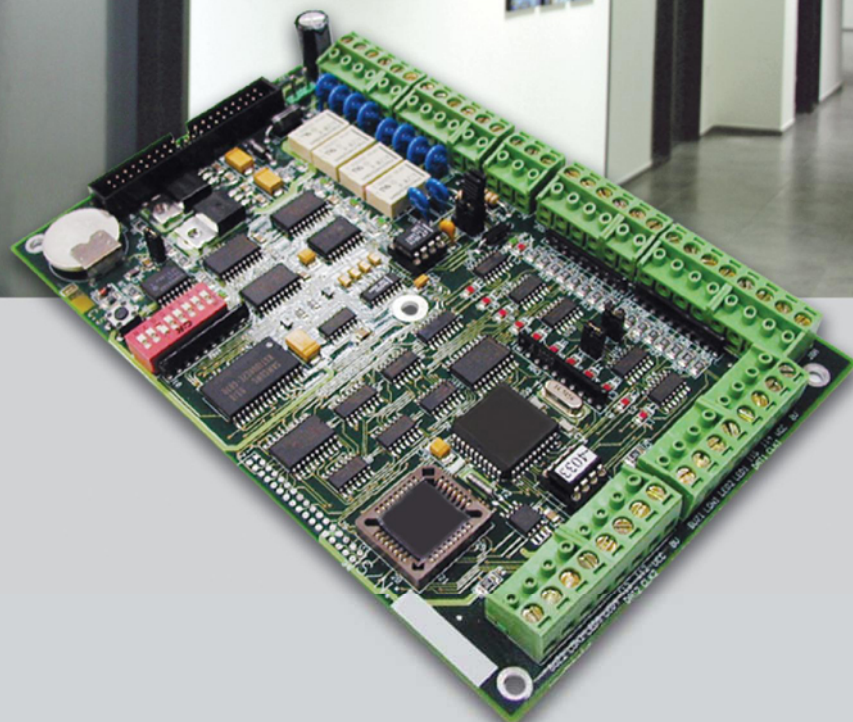
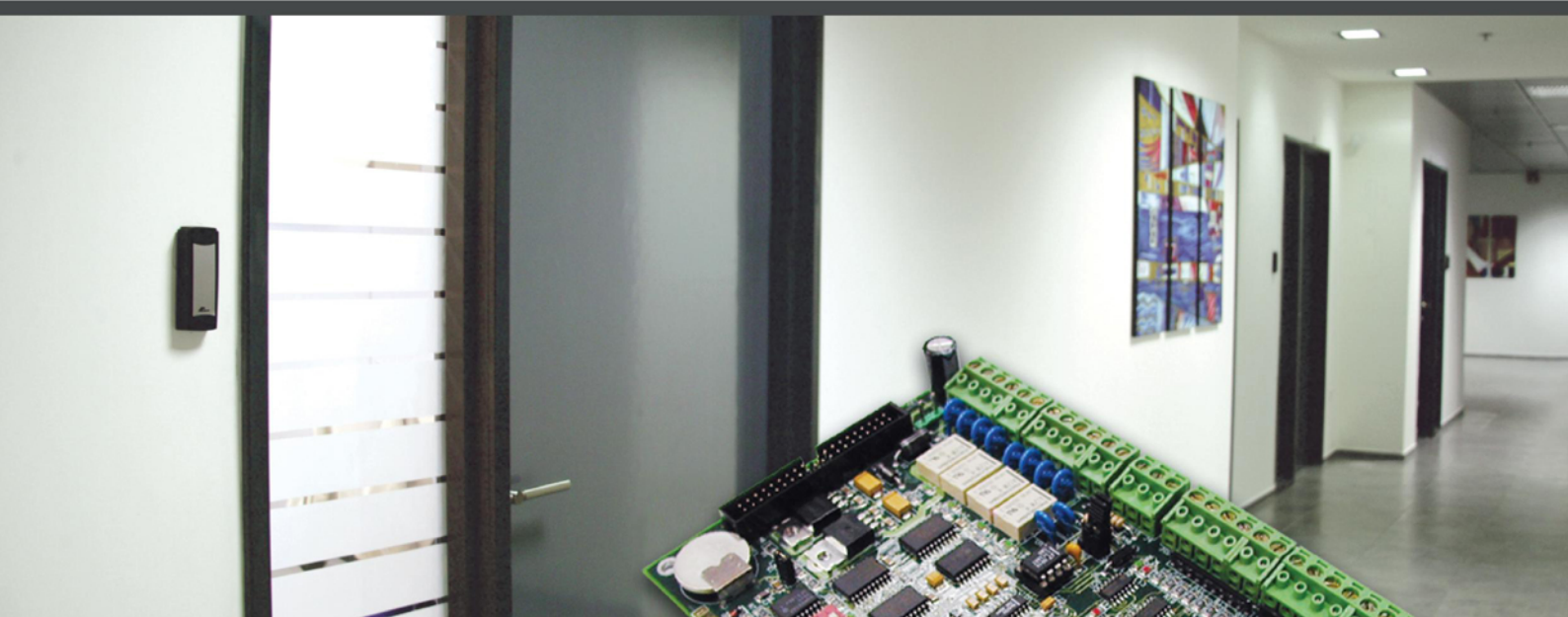


# *ProNet*

## User Manual



# Table of Content

|  |           |
|--|-----------|
| <b>1. WELCOME.....</b>                       | <b>4</b>  |
| 1.1. ABOUT PRONET .....                      | 4         |
| 1.2. MONITORING TOOL .....                   | 4         |
| 1.2.1. Access Control .....                  | 4         |
| 1.3. TYPES OF INSTALLATIONS .....            | 5         |
| 1.4. MODULES .....                           | 5         |
| 1.4.1. Database .....                        | 5         |
| 1.4.2. Communication .....                   | 5         |
| 1.4.3. Operation .....                       | 5         |
| 1.5. BASIC CONFIGURATION.....                | 5         |
| 1.5.1. Operating System and Computer .....   | 5         |
| 1.5.2. Controllers .....                     | 6         |
| 1.5.3. Readers .....                         | 6         |
| 1.5.4. Other Materials.....                  | 6         |
| 1.6. GENERAL USE OF PRONET .....             | 6         |
| 1.6.1. First Installation .....              | 6         |
| 1.6.2. Demonstration Version .....           | 7         |
| 1.6.3. Running ProNet .....                  | 7         |
| 1.6.5. Modifying Data Entry .....            | 7         |
| 1.6.6. New Data Entry.....                   | 8         |
| 1.6.7. Exiting the Application.....          | 8         |
| 1.6.8. Update an ProNet version.....         | 8         |
| 1.6.9. ProNet Database Protection.....       | 9         |
| <b>2. GENERAL SCREENS .....</b>              | <b>9</b>  |
| 2.1. MAIN SCREEN .....                       | 9         |
| 2.2. TOOL BAR .....                          | 10        |
| 2.3. NAVIGATION BAR .....                    | 10        |
| 2.5. PERSONALIZED NAVIGATION BAR .....       | 11        |
| <b>3. “PARAMETER” MENU.....</b>              | <b>11</b> |
| 3.1. CONTROLLER NETWORK .....                | 11        |
| 3.1.1. Controller Network - General.....     | 11        |
| 3.1.2. Controller Network - Definition.....  | 12        |
| 3.2. Controller.....                         | 15        |
| 3.2.1. Controller - General .....            | 15        |
| 3.2.2. Controller - Readers .....            | 16        |
| 3.3.3. Controller - Input .....              | 29        |
| 3.3.4. Controller - Output .....             | 31        |
| 3.3.5. Controller - Local Reflexes.....      | 33        |
| 3.4. TIME ZONE.....                          | 35        |
| 3.4.1. Basic Concepts.....                   | 35        |
| 3.4.2. Daily Program .....                   | 36        |
| 3.4.3. Weekly Program.....                   | 37        |
| 3.4.4. Holiday.....                          | 38        |
| 3.5. ACCESS GROUP .....                      | 39        |
| 3.6. DEPARTMENT .....                        | 40        |
| 3.7. BADGE .....                             | 41        |
| 3.7.1. Badge Search .....                    | 43        |
| 3.7.2. Group of Badges .....                 | 44        |
| 3.8. ALL CARDHOLDERS.....                    | 46        |
| 3.8.1. All cardholders - Basic Concepts..... | 46        |
| 3.8.2. All cardholders - General .....       | 46        |

|  |           |
|--|-----------|
| 3.9. VISITOR.....                              | 52        |
| 3.10. AUTHORIZATION LEVELS .....               | 53        |
| 3.11. USER .....                               | 54        |
| 3.12. LOG OFF.....                             | 55        |
| 3.13. EXITING THE APPLICATION .....            | 55        |
| <b>4. “EVENT HANDLING” MENU.....</b>           | <b>55</b> |
| <b>4. “EVENT HANDLING” MENU.....</b>           | <b>56</b> |
| 4.1. ICON .....                                | 56        |
| 4.2. MAP .....                                 | 57        |
| 4.2.1. Map - General.....                      | 57        |
| 4.2.2. Map - Icon.....                         | 57        |
| 4.3. POSITION .....                            | 58        |
| 4.4. ACTIVE ALARMS .....                       | 59        |
| 4.4.1. Active Alarms - Basic Concepts.....     | 59        |
| 4.4.2. Active Alarms - Map .....               | 60        |
| 4.4.3. Active Alarms - Input Status .....      | 64        |
| 4.4.4. Active Alarms - Output Status.....      | 66        |
| <b>5. “MODULES” MENU .....</b>                 | <b>67</b> |
| 5.1. TIME & ATTENDANCE MANAGEMENT MODULE ..... | 67        |
| 5.1.1. Roll Call.....                          | 67        |
| <b>6. “COMMUNICATION” MENU.....</b>            | <b>68</b> |
| 6.1. DIAGNOSE .....                            | 68        |
| 6.2. VIEW / CLEAR LOG.....                     | 70        |
| 6.3. DISPLAY PHOTO .....                       | 71        |
| <b>7. “TOOLS” MENU.....</b>                    | <b>71</b> |
| 7.1. REPORT WIZARD.....                        | 71        |
| 7.2. CREATE NEW DATABASE .....                 | 74        |
| 7.3. SAVE DATABASE.....                        | 75        |
| 7.4. RESTORE DATABASE .....                    | 75        |
| 7.5. CREATE NEW JOURNAL.....                   | 76        |
| 7.6. SAVE JOURNAL.....                         | 77        |
| 7.7. RESTORE JOURNAL.....                      | 78        |
| 7.8. CREATE A GROUP OF BADGES .....            | 79        |
| 7.9. OPTIONS .....                             | 79        |
| 7.9.1. Files Location .....                    | 80        |
| 7.9.2. Language.....                           | 80        |
| 7.9.3. Communication.....                      | 81        |
| 7.9.4. Journal / Log Screen.....               | 82        |
| 7.9.5. Menu.....                               | 83        |
| 7.9.6. General .....                           | 84        |

# **1. WELCOME**

## **1.1. About ProNet**

The CROW ProNet, the sophisticated yet user-friendly access control and alarm management software, centralizes security requirements within all types of installation irrespective of their complexity.

ProNet offers intelligent and flexible access control that manages cardholders' information, time zones, access levels and relays activation. Controllers and badge holders are automatically created with a click of a mouse. The set-up process is therefore reduced to minutes instead of hours.

ProNet alarm management module monitors all alarm events and movements in real time. All the information needed to react immediately with full knowledge of the facts is provided on the screen. Security is reinforced as alarm conditions and events automatically trigger predefined reactions: flashing icons on relevant displayed maps, written and vocal instructions, alarms, CCTV or any programmed relay activation, zone on/off alarm, card invalidation, etc.

ProNet transforms your facility into a smart building. The passage of a badge at the exit automatically switches off the lights and heating in any designated area, thus allowing for energy savings. Switching on the heating in the office of the person who has passed its badge at the car park entrance.

## **1.2. Monitoring Tool**

### **1.2.1. Access Control**

Access Control tool allow you to define "who is going where and when". Smart multi-technology controllers, linked to advance identification systems, allow to equip each person with a personalised card or another ID that controls access.

Your organization can prevent material or information robbery, by limiting / supervising the access to all or part of your facility (lab, computer room, or storage areas) to authorized persons, during specific time periods.

When a badge holder requests permission to access a particular area, the information is relayed from the reader to the controller. The controller either grants or denies access according to the parameters defined (access authorization, time zones, etc.) All these parameters are down-loaded from the central station (through ProNet) to the controllers into authorization tables and therefore, controllers decide by themselves to grant or deny access, without involving the central station. The transactions are then sent to the central station and listed in the log and the journal.

Access control parameters are mainly defined in the "Parameter" section of the application.

### 1.2.2. Time & Attendance Management

Time & attendance management facilitates the computation of employee attendance, overtime, absences and lateness. It allows calculating pay slips more efficiently.

Time & attendance parameters are mainly defined in the "[Roll call](#)" menu of the "Modules" section of the software.

## 1.3. Types of Installations

ProNet centralizes security within any type of on-line installation:

- Big or small installation
- TCP/IP, RS485 or modem networks
- Single or remote sites

## 1.4. Modules

### 1.4.1. Database

The database module allows creating and modifying databases (reader, systems, badge holders, time zones, etc.)

As soon as a data is created or modified, it is recorded in a file, which is then sent to the controller via the communication module.

Database parameters are defined in the "[Create](#)", "[Save](#)" and "[Restore Database](#)" screens in the "Tools" section of the application. Similar options exist for the journal.

### 1.4.2. Communication

The communication module coordinates the data transfer between the main computer and the controllers that detect the events. The information collected is recorded in the journal and displayed in the log.

### 1.4.3. Operation

The operational module interprets information collected by the communication module. Its role is to activate predefined tasks such as alarms, reflexes, etc.

The events to consider, and the resulting actions, are specified in the different screens of the "Event Handling" section.

## 1.5. Basic Configuration

### 1.5.1. Operating System and Computer

#### Operating system:

Windows 2000 Pro or Windows XPRO or Windows 2003 Server

The manufacturer recommends these two operating systems and is not responsible for errors occurring while using other operating systems.

#### Computer:

Pentium IV minimum

256 MB RAM (or 1 GB RAM for installations with more than 100 controllers or with SQL Server)

500 MB free hard disk space

CDROM Drive

1 free serial COM port and 1 parallel port or USB port

**Recommended enhancement:**

Sound Card , Speakers , SVGA definition (800\*600)

**1.5.2. Controllers**

All CROW controllers for on-line networks are compatible with ProNet.

**1.5.3. Readers**

The vast majority of readers available on the market are compatible with the ProNet system: magnetic, proximity, bar code, smart card, biometry, Wiegand, contact, infrared, keypad, etc.

Consult with your ProNet reseller for further information.

**1.5.4. Other Materials**

In order to successfully install and run the ProNet system, other materials are required. These vary according to each installation: computer network, devices to open doors, alarm detectors, etc. Consult with your ProNet provider for further details.

Note: This product uses software developed by Spread Concepts LLC for use in the Spread toolkit. For more information about Spread see <http://www.spread.org>.

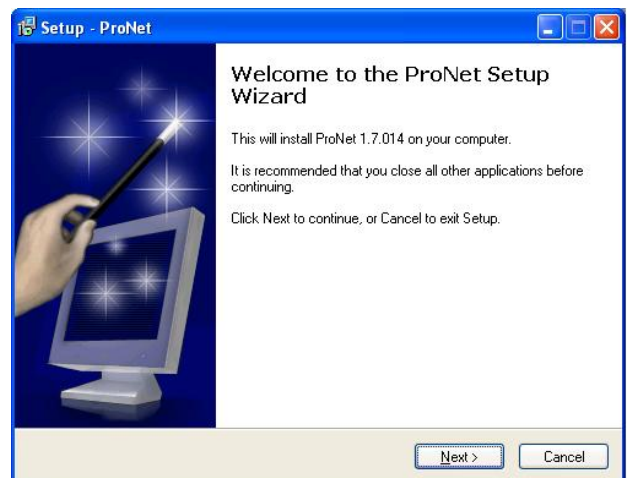
**1.6. General Use of ProNet****1.6.1. First Installation**

Insert the ProNet Installation CD: the Installation Wizard is automatically launched. If not, run the 'autorun.exe' file in the 'autorun' folder of the ProNet Installation CD.

Follow then the step by step instructions.

Note: Do not install the application using the 'setup.exe' file of the CD; should you do so, the following warning message will be displayed:

"Setup will not start. Contact your vendor".

***ProNet on Server/Workstation architecture:***

During the installation, the user is asked to select if the application must run as a Server or as a Workstation. If ProNet runs on one computer only, select 'Server'. If on several computers (for a Server/Workstations architecture), do as follows:

- 1- Install ProNet on the computer that will be the Server and specify 'Server' during the installation process.
- 2- Share the ProNet folder to the required Workstation(s).
- 3- Once installed, run the application and define all the computers, Server and Workstation(s), through the '[Parameter - Computer](#)' screen.
- 4- Install ProNet on each workstation and specify 'workstation' during the installation process. It will ask the user to select the Server network path.

### **Database type:**

During the installation, the user is asked to select the database format: 'Access' or 'SQL'. Select Access Mdb (SQL isn't supported by ProNet).

### **1.6.2. Demonstration Version**

A demo version of the ProNet software is available. It includes all functions referring to alarms, graphics, lift management and time management. Nevertheless the capability of the demo version is restricted to two controllers, four readers and ten cardholders. In order to exceed these capabilities and to use the software in a real situation, a plug is requested.

### **1.6.3. Running ProNet**

Start the ProNet application by double-clicking on its shortcut or by clicking on Start/Programs/ProNet/ProNet from Windows Desktop. Type the User name and the Password and click OK. The application main menu appears on the screen.

### **Tips & Notes**

#### **Significance of lower case and capital letters**

The "User name" and "Password" fields notice the difference between lower case and capital letters. For example: the computer will interpret AFI, afi, and aFi differently.

#### **Three attempts**

If the user name and the password are not correctly entered after three attempts, the start window will disappear from the screen.

#### **Using the software for the first time**

It is recommended to change the user name and the password at the first use of ProNet and to store this information in a secure place.

#### **Skip the user name and password request**

Start your application without being prompted for a user name and a password every time the application is started, by setting them in the initialisation parameters, as follow:

- Point the mouse to the shortcut of the application
- Press on the right click of the mouse
- Select "Properties"
- Add the user name and password at the end of the "Target" field (after "ProNet5.exe") as follow: [space]/us:user name [space]/pw:password
- Click OK

### **1.6.5. Modifying Data Entry**

To modify an existing entry:

- Select the desired screen
- Choose a data entry
- Modify the fields (Choose self-explanatory names)
- Click on the "Save" icon from the navigation bar to confirm the modification of the data captures
- Click on the "Close" icon to terminate the data entry operations and to return to the general screen or click on the "F12" function key.



### 1.6.6. New Data Entry

To create a new data entry:

- Select the required screen
- Click on the “New” icon from the navigation bar, to create a new data entry
- Give a name to the new data entry in the field entitled “Name” (Choose self-explanatory names)
- Define the new data entry in the field entitled “Description”
- Fill in the other fields
- Click on the “Save” icon from the navigation bar to confirm the creation of the data or press the “F3” function key
- Click on the “Close” icon to terminate entry operations and to come back to the general screen or press the “F12” function key


### Tips & Notes

#### Emptying fields

By clicking on the “New” icon all the fields are cleared away or set to their default value to allow new data entry.

### 1.6.7. Exiting the Application

In order to terminate a work session and exit the application, choose one of the following steps:

- Click on the “Exit” icon represented by a door, at the far right of the navigation bar
- Double-click on the icon represented by a magical wand, in the upper left corner of the screen
- Click on the cross , in the upper right corner of the screen
- Click on the “F4” function key and, at the same time, on the “Alt” key
- Open the “Parameter” menu and choose the “Exit” option (at the bottom of the list)

The system offers the possibility to log off unauthorized users, without closing the application.

### 1.6.8. Update an ProNet version

To update an application already installed, do one of the two following procedures:

#### 1- Using an ‘Update’ file:

Exit the application and run the ‘Update’ file (for example: ‘update\_v1.3.023.exe’). Run it on the Server and on each Workstation.

#### 2- Using a full new version of ProNet setup:

2.1 From ProNet, save the database and the journal from the [‘Tools – Save database’](#) and [‘Tools – Save journal’](#) menus.

2.2 Save the ‘ProNet5.ini’ file from the ProNet folder.

2.3 Uninstall ProNet from the computer.

2.4 Install the new version in the same folder where the previous version was installed.

2.5 Copy the saved ‘ProNet5.ini’ file in the ProNet folder, overwriting the existing file.

2.6 Enter the application. If the database and the journal have not been automatically restored by the process, restore them from the [‘Tools – Restore database’](#) and [‘Tools – Restore journal’](#) menus.



### 1.6.9. ProNet Database Protection

In the application folder there is a utility that allows password protection to the main database (ProNet5.mdb). This protection prevents opening the database using Microsoft Access or any other application. To protect the database, follow the next steps:

Operating Mode :

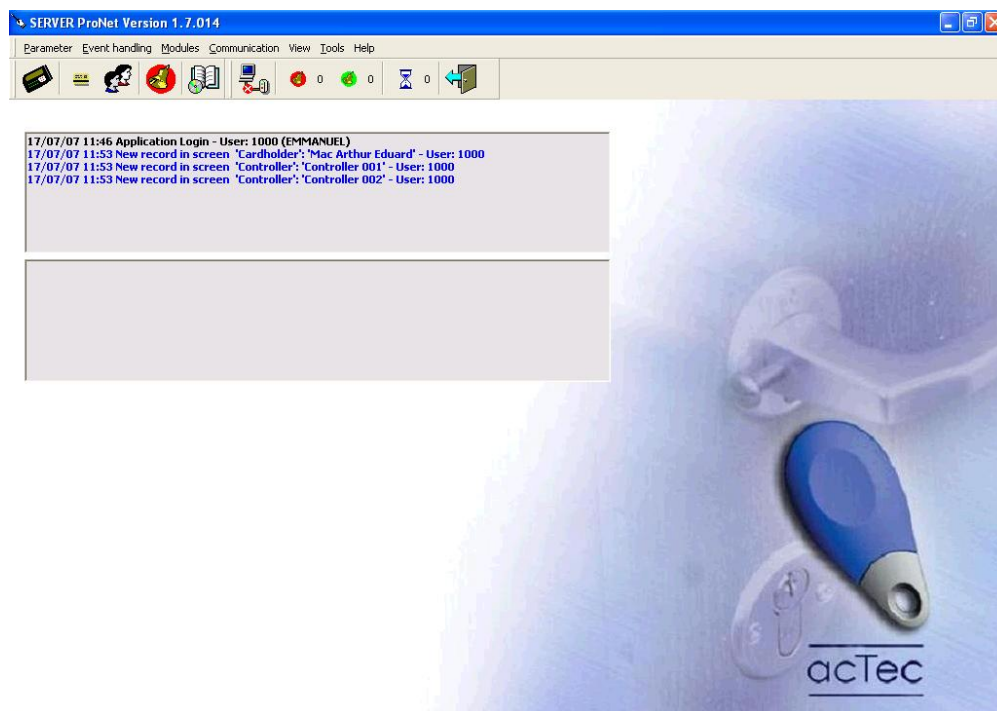
- Exit ProNet,
- Run 'LockDB.exe' from the main application folder,
- Click on 'Select Database' to select the main db (ProNet5.mdb),
- Click on 'Lock Database'.

## 2. GENERAL SCREENS

### 2.1. Main Screen

The main screen of ProNet allows an access to all system options through the use of:

- Scrolling menus, leading to all capture screens, information tables and system options
- Toolbar, providing shortcuts towards some important screens
- Log display, presenting the list of events in real time
- Progress bar, at the bottom of the screen, showing the current status of the commands.



### Tips & Notes

#### Tutorial

The help screen is available from any screen by pressing the “F1” function key and displays explanations of the current screen.

#### Reminding of consulted screens

The fields of the scrolling menus in the main screen appear in **black** before use. However after consultation, they appear in **blue**.

#### Multi-Windows

Several windows can be opened simultaneously.

## Authorization Level

The options displayed depend on the authorization level of the user. Certain options are not suitable for certain users and therefore do not appear on the screen.

## Dissociating the alarm log from the access log

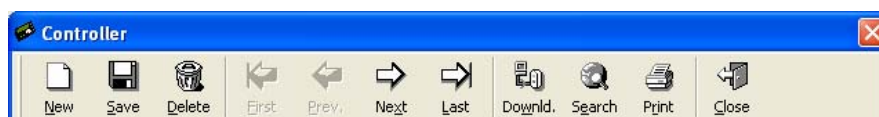
By default, a single log shows access, alarms and system messages. It is possible to dissociate the alarm log from the access log, in the "[Options – Tools – Journal / Log screen](#)" screen.

## 2.2. Tool Bar

The icons of the toolbar provide shortcuts to some important screens: Controller, Badge, All cardholders, Event handling program, Active alarms, Report wizard, Polling, Number of active alarms, Number of acknowledged alarms, Number of pending commands to be sent, Exit.



## 2.3. Navigation Bar



The function keys correspond to the icons on the navigation bar are described here after. They are available from each capture screen.

|     |          |  |
|-----|----------|--|
| F2  | New      | Define a new data entry  |
| F3  | Save     | Save the current data information  |
| F4  | Delete   | Delete the data selected   |
| F5  | First    | Select the first data entry of the list  |
| F6  | Previous | Select the previous data entry   |
| F7  | Next     | Select the next data entry   |
| F8  | Last     | Select the last data entry of the list   |
| F9  | Download | Transfer all the parameters to the corresponding controllers even if the information has not been modified |
| F10 | Search   | Look for the desired data in the list  |
| F11 | Print    | Generate automatically the report corresponding to the current data  |
| F12 | Close    | Close the screen and return to the previous screen   |

## Tips & Notes

### Tutorial

|    |      |   |
|----|------|---|
| F1 | Help | Display the help screen of the current screen |
|----|------|---|

### New Data

By clicking on the F2 key, the fields of the newly created item are empty to allow entry of new data. If existing information has not yet been saved, a message appears requesting the user to save or cancel the changes. Saving (F3 key) transfers automatically the modified parameters to corresponding controllers.

## 2.5. Personalized Navigation Bar

A customized toolbar gives added flexibility to the system.

### Creating a customized toolbar

- Place the mouse on the original toolbar
- Click on the mouse right button
- Select “Customize” in the menu that appears on the screen for opening the [tools screen](#)
- Click on the "New" button and give a name to the new toolbar
- In the “Tools” tab, select the desired group of icons
- Select the tools in the list and drag and drop them on the new toolbar

### Saving a customized toolbar

Check the box “Save user customized toolbar” in the “[Tools – Options – General](#)” screen for restoring the customized toolbar at each work session.

### Toolbar initialisation

To execute this command, click on the “Reset toolbar to original state” button in the “[Tool - Options - General](#)” screen.

## 3. “Parameter” MENU

### 3.1. Controller Network

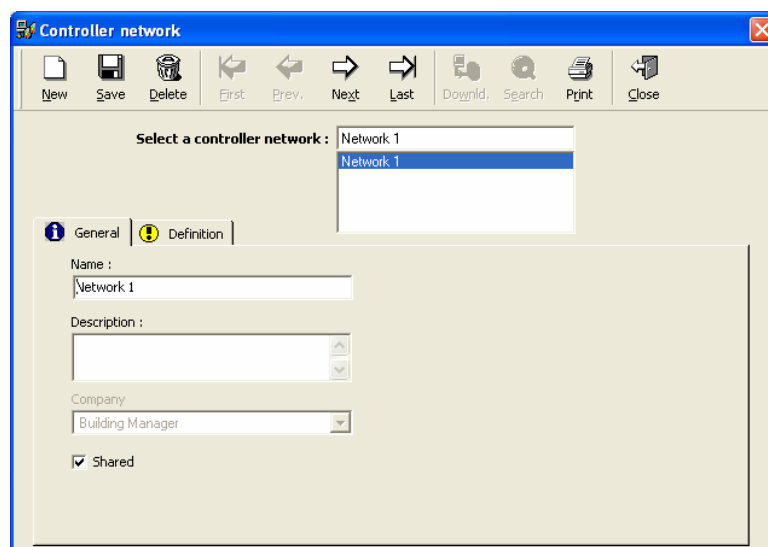
A network is an electrical physical support - or bus - to which controllers are connected and which can be connected to a PC. The different networks, to which groups of controllers are connected, are defined in this screen.

The PC can be connected to the networks by its communication ports (one by network), by its Ethernet TCP/IP board (for LAN or WAN network) or by Modem.

The controller network parameters are divided into two tabs:

- [General](#), for name and description
- [Definition](#), for selection of the different parameters

#### 3.1.1. Controller Network - General



The screenshot shows a window titled "Controller network" with a standard Windows-style toolbar at the top containing icons for New, Save, Delete, First, Prev., Next, Last, Download, Search, Print, and Close. Below the toolbar, there is a section labeled "Select a controller network:" with a list box containing "Network 1". Below this, there are two tabs: "General" (selected) and "Definition". The "General" tab contains the following fields: "Name:" with a text box containing "Network 1", "Description:" with a text box, "Company:" with a dropdown menu showing "Building Manager", and a checked checkbox labeled "Shared".

### Fields

**Name:** Name the new network

**Description:** Describe the new data entry

**Company:** Company the item refers to (for use with multi-company application ONLY).

**Shared:** Check the box for sharing the information between different companies (for use with multi-company application ONLY).

### 3.1.2. Controller Network - Definition

Three network types are recognised by the system: Port COM, Port TCP and Port MODEM.

For each kind of network the following fields may be defined:

**Password:** This password allows to secure the data traffic between the PC and the controllers by encoding the information that passes over the communication bus (whether serial or TCP/IP). Each controller network may have a user defined 32-bit password, written in hexadecimal characters. When the PC and the controllers communicate, each data packet is encrypted using this password, preventing a hacker that has a copy of ProNet application from accessing the controllers. The password can be defined after checking the 'Password' box in this screen. The user can use decimal digits or a combination of decimal and hexadecimal characters.

Example: 1A E3 5F 7B (Min. value: 01 00 00 00 / Max value: 7F FF FF FF)

**Time out delay:** The maximum delay, measured in milliseconds, beyond which a controller must answer to a command sent by ProNet. If the controller does not answer within this delay, ProNet will try two more times (value adjustable in the '[Tools – Options – Communication](#)' menu) to send the command. If still no answer from the controller, the command will be put in the pending commands. The default value is 1000 msec. (keep this value unless specified otherwise)

**Time out polling:** Polling a controller means asking it if some events just occurred, i.e. either a card transaction (granted or denied) or an alarm. In the polling mode, ProNet continuously polls all the controllers which must answer either by an empty message, if nothing happened, or by the last event(s) occurred. The 'Time out polling' is the maximum delay, measured in milliseconds, beyond which a controller must answer to a polling. If the controller does not answer within this delay, ProNet will try two more times to poll it. If still no answer from the controller, it will jump to the next controller. The default value is 1000 msec. (keep this value unless specified otherwise)

ProNet will declare a Communication problem if a same controller does not answer to polling during a pre-defined 'communication error time-out' delay.

The number of trials (3 by default) ProNet will poll a controller which does not answer and the 'communication error time-out' delay (30 seconds by default) is adjustable in the '[Tools – Options – Communication](#)' menu.

**Waiting delay:** Specify the delay between two communication operations between the computer and the controllers (polling or commands) - measured in milliseconds. This function will help slow down the system so as to free up the PC. The default value is 50 msec. (keep this value unless specified otherwise)

Note: The communication baud rate between controllers and ProNet is defined in the '[Tools – Options – Communication](#)' screen.

### 3.1.2.1. COM Network

#### Fields

**Port:** Choose “COM” and specify the port address; by default the serial port COM 1 is created.

The screenshot shows the 'Controller network' dialog box with the 'General' tab selected. The 'Select a controller network' list shows 'Network 1'. The 'Port' dropdown is set to 'COM' and the port number is '1'. The 'Password' checkbox is checked. The 'Time out delay' is 1000 Msec, 'Time out polling' is 1000 Msec, and 'Waiting delay' is 500 Msec.

### 3.1.2.2. TCP Network

#### Fields

**Port:** Select “TCP” to establish a link to remote controllers via TCP/IP

**Phone No. or TCP address:** Specify the TCP address requested in the format <Address>:<Port>, for example: 10.0.0.1:10001

The screenshot shows the 'Controller network' dialog box with the 'General' tab selected. The 'Select a controller network' list shows 'Network 1'. The 'Port' dropdown is set to 'TCP'. The 'Password' checkbox is checked. The 'Time out delay' is 1000 Msec, 'Time out polling' is 1000 Msec, and 'Waiting delay' is 500 Msec. The 'If remote or TCP' section is expanded, showing a text field for 'Phone no. or TCP address' with the instruction: 'for TCP put <Address>:<Port> such as 10.0.0.1:1001'.

### 3.1.2.3. Modem Network

#### Fields

**Port:** Select “Modem” to establish a link to remote controllers via modem

**Phone No. or TCP address:** Specify the phone number of the modem requested

**Modem:** Select the required modem among the drop-down list showing the current Windows pre-defined connections.

The screenshot shows the 'Controller network' dialog box with the 'General' tab selected. The 'Select a controller network' list shows 'Network 1'. The 'Port' dropdown is set to 'MODEM'. The 'Password' checkbox is checked. The 'Time out delay' is 1000 Msec, 'Time out polling' is 1000 Msec, and 'Waiting delay' is 500 Msec. The 'If remote or TCP' section is expanded, showing a text field for 'Phone no. or TCP address' and a 'Modem' dropdown menu with two modem icons below it.

Note:

- Set the remote modem in auto answer mode
- Fit the specific wiring and settings to installation instructions of controllers
- Establish modem port selection at the server

**Connect:** Click on the connect button to start the connection procedure; this button is enable after saving the network definition only.

The server application will show messages such as “Proceeding”, “Line Busy” or “Connected”.

The connect button is available on any workstation of the system, nevertheless the status messages are only sent to the server computer.

**Disconnect:** Click to stop the connection procedure; this button is only enabled while the controller network is connected.

Note: In case of off-line network, all the controllers are considered as inactive by the system. Database modifications are saved and automatically transferred during the next successful connection.

## Tips & Notes

### **Updating dial up controllers**

When a remote controller network is connected via dial up modem, and the user makes changes in the database while these networks are not connected, there are 3 ways of updating controllers with the new definitions:

**1. Manually:** Open [Controller Network](#) screen and connect to the relevant network. Once connected, all pending commands are sent to the controller, and in addition, the events buffer is uploaded to the PC.

**2. By user defined schedule:** Modem dial-up may be automatically performed within pre-defined schedules. Define a new action and select the type: “Connect distant network and read transactions”. Select the relevant remote controller network. Save. Click “Make it a process”. Define a new global reflex. Select the type “Scheduler” and select the relevant time and dates. For example: Any day, any month, at 23:00. Select the newly created process. Save. This will make the program dial up that modem every night at 23:00, update the pending commands, read the events, and disconnect.

**3. Automatic dial up every time there pending are to be sent:** When a local controller does not answer to controller commands, (usually due to a communication problem), these commands are left as pendings and sent, by default, every half an hour minutes. (That 30 minutes period may be changed, down to a minimum of 1 minute, though [Tools - Options - Communication - Resend pending every...](#)). In order to set the application to update pendings, (at the same method and at the same delay), also remote dial up networks, it is required to choose the “Distant connect on pending” option in the [“Tools - Options - Communication”](#) screen.

Note: When this option is activated, the AM5 would not dial up every pending updates period to all remote controllers, but only to those who have to be updated with database changes. Therefore, if a certain controller does not have to be updated, AM5 will not connect to it and would not empty its buffer. (See the [paragraph which explains what happens when buffer is full on remote controller](#)).



### 3.2. Controller

A controller is an electronic card that has a huge memory capacity for storing the parameters monitored, such as cardholders, time zones, reflexes, etc. It supervises the following components of the security system:

- Readers, and consequently the corresponding doors
- Inputs (Alarm, RTX buttons, etc.)
- Outputs relays

Information regarding controllers is organized into 5 tabs:

- [General](#) tab
- [Readers](#) tab
- [Input](#) tab
- [Output](#) tab
- [Local reflexes](#) tab

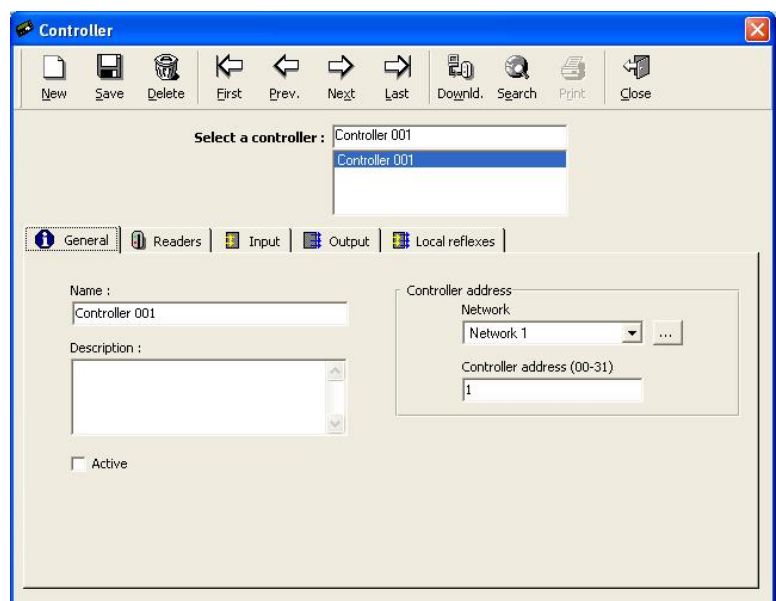
#### 3.2.1. Controller - General

The “Parameter - Controller - General” menu allows to define the controller parameters in the system.

##### Fields

**Name:** The following names appear by default: Controller 1, Controller 2, etc. Modify the default name by a name linked to the geographical position of the controller or to the department it monitors. In case the controller monitors many readers at a time, the name chosen must be logical. Examples: main entrance, stairs –1, parking 2, R&D

**Description:** Describe the new data entry



**Active:** ☒: to activate communication (parameters download and polling) with the controller.  
☐: to disengage communication between the PC and the controller. Polling is not done in this case; the controller is not polled and is not downloaded by the system.

**Set as default:** Check the box if the current controller should serve as a reference. Its parameters are automatically copied as default parameters for newly created controllers, thus preventing to have to parameter newly created future controllers.

**Company:** Company the item refers to (for use with multi-company application ONLY).

##### **Controller address:**

**Network:** Select an existing network from a list of previously defined networks or create a new network by clicking on the [...] button.

**Controller address (00-31):** Mention the physical address of the controller in the selected network. The address is contained between 00 and 31; it is defined on the controller itself by the position of the address selection dip switches.



### 3.2.2. Controller - Readers

The informative table synthesizes reader parameters that are associated to a controller. Default parameters are defined according to the type of controller. To obtain full information and modify the reader data, click on the [...] button situated to the right of the table of the corresponding tab.

#### Table analysis

**Name:** Reader name

**Door alarm:** Name of the input signalling the closure of a door

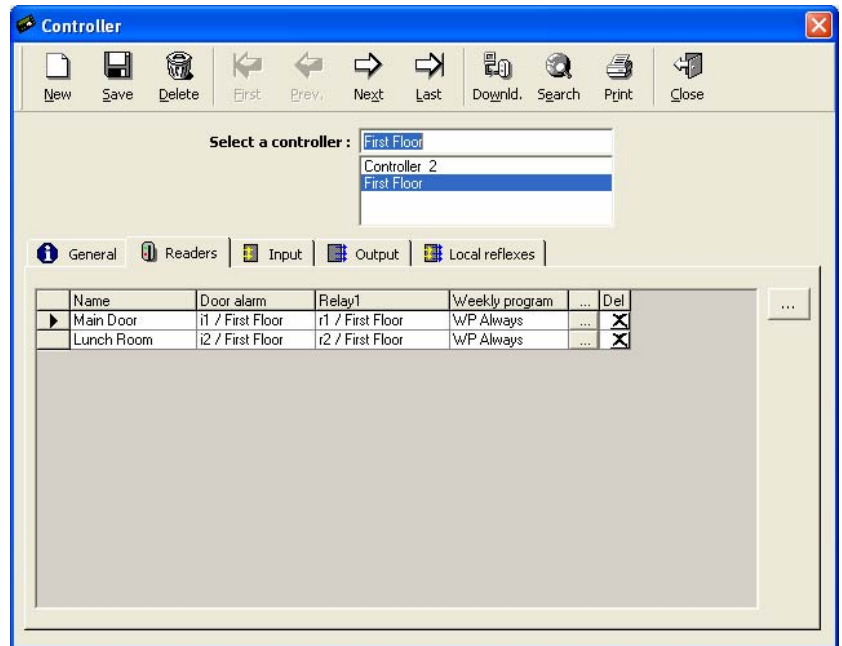
**Relay 1:** Name of the first output in the system

**Weekly program:** Weekly program that automatically flip-flops the way the reader operates between the two security levels

**Button [...]** (on the line of the reader): Click on the button to display the “[Reader](#)” screen for creating, consulting or modifying data

**Button [x]** (on the line of the reader): Click on this button to remove a reader from the line

**Button [...]** (outside the table): Click on the button to display the “[Reader](#)” screen even if no record is selected



#### Tips & Notes

##### **Modifying default parameters**

Suppress readers that automatically appear in the table and are not physically connected. If the default parameters of a reader are not suitable, eliminate the reader from the list and manually create a new data entry. In case of an empty list, click on the [...] button to create a reader.

##### **Saving current information**

As soon as a new tab is selected all the current information is saved.

#### Table of default connections for inputs, relays and RTX:

|            | Reader 1 | Reader 2 | Reader 3 | Reader 4 |
|------------|----------|----------|----------|----------|
| Door alarm | i1       | i2       | i5       | i6       |
| Door relay | r1       | r2       | r3       | r4       |
| RTX        | i3       | i4       | i7       | i8       |

### 3.2.2.1. Controller - Readers - General

The “Reader” screen enables the reader parameters specification. It is accessible from the corresponding tab in the “Controller” screen, by pressing on the [...] **button** situated to the right of the table.

Reader parameters are divided into five categories:

- [General](#) tab
- [Door control](#) tab
- [Access mode](#) tab
- [Miscellaneous / Badge format](#) tab
- [Finger Print](#) tab (if a biometric reader is selected)

#### Fields

**Name:** Name the reader

**Number:** Indicate the number of the reader (choose from 1 to 2 for a two doors controller, and from 1 to 4 for a four doors controller).

**Shared:** Check the box for sharing the information between different companies (for use with multi-company application ONLY).

**Description:** Describe the new data entry

**Camera:** Select the camera video to associate with this reader, if needed (for use with the [Video Module](#) ONLY).

**Company:** Company the item refers to (for use with multi-company application ONLY).

**Has a slave reader:** Check the box; if checked, specify the name of the slave reader.

**Note:** When a reader is deleted its slave reader is also deleted.

**Technology:** Select the reading technology from the displayed list (Magnetic, Wiegand, etc.)

The information downloaded to the readers is limited to the badges which have the same technology as specified above. The badge technology is specified in the “Type” field in the [“Parameter - Badge”](#) screen.

**Note on Badge Technology:** A badge, or card, is a physical support that has a unique code enabling its identification. Generally, this code is randomly attributed and unknown to the user. Badges identification requires the registration of their code in the system memory. When a badge is being read the system checks if the badge is known and if yes, to whom it is attributed, for checking the access authorization of the cardholder.

Numerous card technologies are available: magnetic, bar code, Wiegand, proximity, smart cards, etc. ProNet, as well as CROW controllers, is compatible with the majority of reader technologies on the market today.

The reading technology is defined in the “Controller – Reader - General” screen and badges technology is defined in the [“Parameter - Badge”](#) screen. The technology must be the same as the one selected on the controller electronic board through its technology selection jumpers.

**Biometrics:** If the reader is a biometric reader, select its type from the displayed list (BioPass, etc.).

## Tips & Notes

### Motorized Reader

It is possible to use the CROW magnetic motorized readers by selecting the 'Motorized Reader' technology in this screen. Two additional fields are displayed: in the first, select the controller input connected to the badge detection signal (S1). In the second, select the controller relay to which the Common is connected to the signal (MFC/MRC) that controls the sense of the reader motor.

### 'Wiegand', 'Wiegand 2' and 'Wiegand Keypad' Technologies

When several readers are defined with a same technology, they must have the same badge format. If some readers need a different format from the current badge format (i.e. a different Wiegand format), their technology must be different and they must be connected on a different controller.

The Wiegand reader technologies ('Wiegand', 'Wiegand 2' and 'Wiegand Keypad') allow to choose up to three different Wiegand format type. This helps for instance on sites where one or more controllers support biometric readers and other controllers support other Wiegand readers.

#### Example:

A site has 2 readers; each one is connected on a different controller:

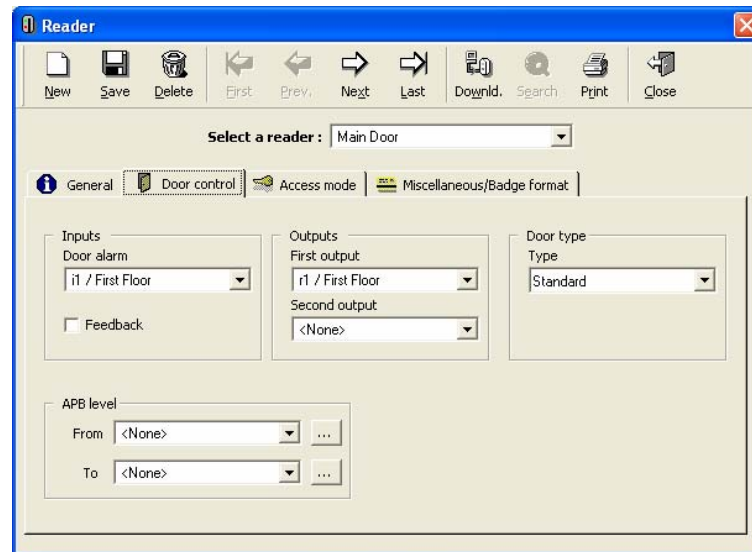
- Reader 1 / Controller 1 is a Bio-pass,
- Reader 1 / Controller 2 is a simple Wiegand reader.

|                         | Defined Technology | Biometrics | Badge Format |
|-------------------------|--------------------|------------|--------------|
| Reader 1 / Controller 1 | Wiegand            | BioPass    | Decimal      |
| Reader 1 / Controller 2 | Wiegand2           | -          | Decimal      |

In this case, if a cardholder needs to pass on **both readers**, he may have **two badges**: one 'Wiegand' badge (to be used on the BioPass reader defined as "Wiegand") and one 'Wiegand2' badge (for the other reader defined accordingly). The PC will download cards of a defined technology only to readers of the same technology. Wiegand cards to Wiegand readers, Wiegand2 cards to Wiegand2 readers, etc.

### 3.2.2.2. Controller - Readers - Door Control

This screen defines the way the door is wired



#### Fields

##### Inputs:

**Door alarm:** Select the controller input to which the door opening control device is wired; an alarm is set off when a door is forced or stays open beyond a predefined delay

**Feedback:** Check the box in order to verify the physical entry or exit of a badge holder that has been granted access

Operation mode: A badge holder swipes his badge through a reader. The controller authorizes access to the badge holder by activating a door relay. During the predefined door alarm delay, during which the door can be opened, the controller goes into a waiting mode. If the door has been opened and closed - as will attest the door opening control device activation - the badge holder is supposed to have passed and the controller records the access transaction in memory. If the door has not been opened, the door opening control device is not activated and the controller records the transaction "access refused" in memory.

**APB level** (for [Global Anti-Passback](#) function):

**From:** Select a reader APB level to be the 'Previous level' of the reader from the list or click on the [...] **button** to define a new APB level

**To:** select a reader APB level to be the 'Actual level' of the reader from the list or click on the [...] **button** to define a new APB level

Operation mode: See the [Global Anti-Passback](#) function in the next paragraph.

##### Outputs:

**First and Second Outputs:** Select the relays to be activated upon a granted access.

**Door type:** Select from the list:

- **Standard:** Access is granted if badge is authorized
- **Controlled by Input:** A door is controlled by the status of an input. Specify the input in question in the 'Controlled by' field. the door opens if the input is inactive but remains closed if the input is active. (If, for example, the input selected is a second door alarm input, the door will be opened only if this second door is closed)
- **Man Trap 1, 3, 4:** Select if the doors operate in the man trap mode, which means that the passage through two consecutive doors is a requisite in order to access a site.
- **Manually Controlled:** Access is manually regulated

### Note on the Mantrap mode:

The man trap mode supervises the activation process of a double door entrance. The first door opening and the possible activation of an input are the conditions for the opening of a second door.

ProNet supervises three types of man traps:

- **Man trap 1:** The first door will open only if the second door is closed. Both readers of a same controller monitor two doors (reader 1 with reader 2 or reader 3 with reader 4). The door of each reader must be defined as 'Man trap 1'. When access is granted at a reader, this reader is locked until the person passes through the second door. The door opening control device status attests to the opening or closure of doors.
- **Man trap 3:** The second door opens automatically following the opening and closure of the first door. Both readers of a same controller monitor two doors (reader 1 with reader 2 or reader 3 with reader 4). The door of each reader must be defined as 'Man trap 3'. When the first door opens and closes the second door automatically opens. The door opening control device status attests to the opening or closure of doors.
- **Man trap 4:** The second door automatically opens consecutively to the following two conditions:
  - Opening and closure of the first door and
  - Receipt of a signal - activation of an input

Both readers of a same controller monitor two doors (reader 1 with reader 2 or reader 3 with reader 4). The door of each reader must be defined as 'Man trap 4'. When the first door opens and closes and a predefined input is activated, the second door opens automatically. The required input must be defined in the 'Controlled by' field. The door opening control device status attests to the opening or closure of doors.

### **3.2.2.3. Controller - Readers - Access Mode**

The reader can operate differently according to predetermined time zones. The parameters of these two operation modes - or security levels - are defined in this screen.

The screenshot shows the 'Reader' configuration window with the 'Access mode' tab selected. The 'Select a reader' dropdown is set to 'Rdr01 / Controller 001'. The 'Weekly program' is set to 'WP Always'. The 'Door remote input' is set to 'i03 / Controller 001'. There are two security levels defined:

| Security level 1                                    | Security level 2                                    |
|---|---|
| With Card   | With Card   |
| <input type="checkbox"/> Anti-Passback              | <input type="checkbox"/> Anti-Passback              |
| <input type="checkbox"/> Free access                | <input type="checkbox"/> Free access                |
| <input type="checkbox"/> Closed if buffer is full   | <input type="checkbox"/> Closed if buffer is full   |
| <input checked="" type="checkbox"/> Door Controlled | <input checked="" type="checkbox"/> Door Controlled |
| Door open time: 4 Sec                               | Door open time: 4 Sec                               |
| Time APB: 0 Min                                     | Time APB: 0 Min                                     |
| Door alarm delay: 10 Sec                            | Door alarm delay: 10 Sec                            |

### **Example**

During office hours, access is freely granted (no need to swipe a badge). After office hours, badges need to be swiped (controlled door).

## Fields

**Weekly program:** Choose the weekly program that automatically flip-flops the reader functioning mode between the two security levels. The default weekly program is always associated with security level Number 1. Click on the [...] **button** to create or modify the weekly program

**Door remote input:** Select the controller input to which the Request to Exit device (RTX) is wired (see in this chapter the [Table of default connections for inputs, relays and RTX](#))

**Security level 1 and 2:** (must be filled out separately for both access modes)

**Access authorization:** Define the way in which the authorization access must be required:

- **With Card**, through the reader
- **With Keypad**, for the entry of a PIN code (Personal identification number)
- **With Card OR Keypad**
- **With Card AND Keypad**

**Anti-Passback & Time APB:** (use with the “Feedback” option)

- **Local Anti-Passback:** The Local Anti-Passback feature provides a mean of stopping a card from being used for successive entries without a valid exit, or vice-versa.

For example, when two readers are connected to control the same door, entrance/exit (Reader 1/3 control entrance/exit of door 1 and reader 2/4 control entrance/exit of door 2), the same card will not be accepted twice successively at the same reader. It has to be passed once at one reader (i.e. entrance) and once at the second reader (i.e. exit). This prevents a person, who has been granted access, to give his card to somebody else that will try to access immediately after the first person.

To activate the Local Anti-Passback, check the Anti-Passback box and leave empty the fields ‘From’ and ‘To’ of the ‘APB level’ in the [‘Reader – Door Control’](#) screen.

- **Time Anti-Passback:** also called “lock out delay”, this feature prevents a card to be granted access twice at a same reader in a pre-defined delay of time. A second access will only be authorized after the lockout delay.

To activate the Time Anti-Passback, fill the ‘Time APB’ field with the lockout delay (between 1 and 15 minutes) as required. For activating in the same time the Local Anti-Passback feature, check the Anti-Passback box.

- **Global Anti-Passback:** defines a path that cardholders must follow to access specific locations. The facilities is divided into levels and each reader allows to pass from a level (“previous level”) to the next one (“actual level”). When the feature is active, the controller will grant access only to cardholders who are coming from the zone classified “previous level”. Once access is given, the cardholder will be located in the “actual level” zone.

***Because the new cardholder level is updated in all controllers by ProNet as soon as it receives the access transaction, the PC must be on-line when this feature is used.***

### Examples:

- Enforce discipline by having cardholders passing through a main entrance checkpoint before they go to their respective offices.
- Prevent a second person (or car) from entering with an authorized one: it will be stopped at the next checkpoint because not registered at the previous level.

To activate the Global Anti-Passback, check the Anti-Passback box and fill the fields ‘From’ and ‘To’ with the previous level and the next level as required, in the ‘APB level’ section of the [‘Reader – Door control’](#) screen.



- **Soft Anti-Passback (requires special controller firmware):** When a cardholder requests to access a second time from a same reader which is defined in Anti-Passback mode, the controller denies the access AND reports the event as “Access Denied - Anti-Passback”. With the Soft Anti-Passback mode, the controller grants the access and only reports the event.

Before setting the Soft Anti-PassBack:

1. Verifying with your vendor that the controller firmware supports this feature.
2. Check the Soft Anti-PassBack box on the “[Tools – Options – Server](#)” screen.

To activate the Soft Anti-PassBack, checking the “Anti-Passback” box will reveal the “Soft” option. Checking that box would apply the Soft Anti-PassBack to that reader. When Soft Anti-PassBack is selected – it applies at ALL times when the Anti-Pass back works, i.e., it is not possible to have full Anti-PassBack on green periods and soft on red periods or vice versa.

**Note:** The Anti-Passback feature may however be cancelled for specific cardholders by selecting the ‘No APB, No timed Anti-Passback’ box in the ‘[All cardholders – Personal](#)’ screen. It can be also re-initialized in the ‘[All cardholders – Location](#)’ screen.

**Free access:** Select to grant unlimited access to all badge holders registered in the system without checking of their validation date or their access group

**Close if buffer is full:** Select this function to refuse access when the corresponding transaction cannot be registered in the system memory, because it is full. If this option is not selected, access is granted even if the buffer is full and, as a consequence, transactions are not recorded.

#### Door mode:

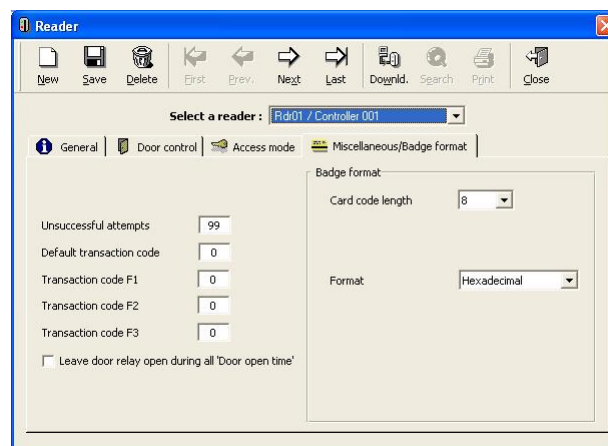
- **Door Open:** Access mode in which the door is permanently open
- **Door Closed:** Access mode in which the door is permanently closed; access is always refused even with valid badges
- **Door Controlled:** Standard access control mode, in which access depends on the badge and its authorizations

**Door open time** (from 0 to 120 seconds): Delay during which the badge holder has to pass through the door after receiving access authorization; it corresponds to the activation delay of the relay(s) which control the door.

**Note:** Alternated mode (Door open time set to 122): The door relay opens after the first valid swipe and stays open; the door relay closes only after a valid second badge reading and stays closed, and so on.

**Door alarm delay** (from 0 to 75 seconds, by multiples of 5): Delay during which the door must be closed; if the door is still open after this delay, a ‘Door left open Alarm’ is raised.

### 3.2.2.4. Controller - Readers - Miscellaneous/Badge Format





## Fields

**Card issue reader:** Select this option to create new badges using a reader. *If the reader is in the card issue reader mode, it cannot be used for access control purposes.*

The card issue reader is generally situated close to the computer. When a badge is read, its code is directly transmit to the PC for recording purpose, without any authorization checks, and this to prevent the small waiting delay this check may take.

**Unsuccessful attempts:** specify the number of successive unsuccessful attempts tolerated by the system before an alarm is raised; choose a number from 00 to 99

**Default Transaction code:** specify the transaction code sent by the controller to the PC when an access is granted; the user via the reader keypad can modify this code

**Transaction code F1, F2, F3:** attribute a specific transaction code to the keypad function keys (if exist). This code is sent when access is granted and the function key was used.

Note: Pre-defined action(s) may be triggered by ProNet upon reception of specific transaction codes. (Refer to '[Global Reflex](#)' Chapter)

**Leave door relay open during all "Door Open Time":** If not selected (by default), the controller deactivates the door relay as soon as it detects (through the door contact device) that the door has been opened. Selecting this option will leave the relay activated during the door open time.

**Badge Format Fields:** There are various formats of magnetic, bar code and Wiegand technologies. By default the system reads the first 8 encoded numbers on magnetic or bar code badges or the 8 hexadecimal digits of a Wiegand badge but this way of reading can be modified. These fields allow to change this badge format.

Controllers may recognize many kind of badge technologies (Magnetic, Barcodes, Wiegand, etc...). The reading technology used must be specified in the '[Controller – Reader – General](#)' screen.

Within a same technology, different formats may be defined through this 'Miscellaneous-Badge format' screen as described hereunder.

### ***Magnetic and Barcode technologies:***

When one of these technologies is selected in the '[Controller – Reader – General](#)' screen, the following fields of the 'Controller - Readers - Miscellaneous/Badge Format' screen may be used to parameter the badge format (Card code position and Customer code, if needed).

## Fields

**System card:** Card on which a four-digit number between 0001 and 9999 has been inscribed; since the card number is already on the badge, it enables immediate recognition of the badge holder and therefore, a system badge need not be recorded up in the system.

**Card code position:** The 'card code' is a unique code, which identifies the card. The system records card code of 8 digits only. A bar code or magnetic code may contain many numbers or characters; by default, the first 8 characters of the code are recorded as the 'card code'. It is possible however to read another 8-digit by specifying the position of the first one in the "Card Code Position" field (Value between 0 and 37, the default value 0 corresponds to the first encoded character).

**Customer (or site) code:** It is a same code, which appears on all the cards of a same company, besides the badge code; the use of a customer code value is optional and strengthens system security by identifying the company.

By the default this option is not used. To use it, fill out the following three fields:

- **Customer code position:** Specify the position of the first character of the code; choose a value between 0 and 37 (0 corresponds to the position of the first number encoded in the badge).
- **Customer code length:** Specify the size of the code to be read; choose a value between 1 and 7. Note that 0 is the default value, which means that the customer code value is not checked.
- **Customer code value:** Enter the customer code value into the squares that appear on the screen.

### ***Wiegand technology:***

When Wiegand technology is selected in the '[Controller – Reader – General](#)' screen, different formats may be selected in the 'Controller - Readers - Miscellaneous/Badge Format' screen.

### **Fields**

- **Hexadecimal:** 'Hexadecimal' format is selected by default. Many standards exist on the market. CROW controllers may read up to 50 bits Wiegand badges (Wiegand codes are read in a binary format), within 48 bits of data (12 hexadecimal digits) and 2 parity bits, as follows:

**E b<sub>47</sub> ..... b b b b<sub>0</sub> O**

Where: **b<sub>47</sub> ... b<sub>0</sub>** = 48 bits of data maximum (may be less) and **E,O** = 2 parity bits

In this hexadecimal format, the system keeps as the 'card code' the 32 least significant bits of the data string (b<sub>31</sub>...b<sub>0</sub>), in other words the last 8 digits of the code, which may be hexadecimal.

Two parity bits are added to the card besides the badge code for confirmation of a proper reading. Most Wiegand standards use a similar algorithm to calculate these parity bits and this algorithm has been integrated into the CROW controllers. It is thus preferable to use it by selecting the corresponding jumpers on the controllers' electronic card.

However, certain card standards have original algorithm for the calculation of the parity bits. In order to enable these controllers to read these badges, the jumper position "no parity bits" must be selected. (See the controller installation manual for further details).

- **Wiegand 44:** 'Wiegand 44' format is a particular format of 44 bits, which includes 40 bits of data (10 hexadecimal digits) and 4 parity bits, as follows:

**b<sub>43</sub> ..... b<sub>4</sub> b<sub>3</sub> b<sub>2</sub> b<sub>1</sub> b<sub>0</sub>**

Where: **b<sub>43</sub> ... b<sub>4</sub>** = 40 bits of data and **b<sub>3</sub> ... b<sub>0</sub>** = 4 parity bits.

In this format, the system keeps as the 'card code' the 32 least significant bits of the data string (b<sub>35</sub>...b<sub>4</sub>), in other words the last 8 digits of the code, which may be hexadecimal.

- **Decimal:** This format is a particular format, where badge code consists on a 5 digits decimal number (generally printed on the badge) sometimes associated with a 3 digits

decimal code site. CROW controllers may read a 50 bits Wiegand string as in the hexadecimal format but convert the information in decimal as follows:

**E b<sub>47</sub> ..... b b b b<sub>0</sub> O**

Where: **b<sub>15</sub> ... b<sub>0</sub>** = 16 bits for 'card code', **b<sub>23</sub> ... b<sub>16</sub>** = 8 bits for 'site code' and **E,O** = 2 parity bits.

In this format, the system keeps as the 'card code' the 16 least significant bits of the data string (b<sub>15</sub>...b<sub>0</sub>), in other words the last 4 hexadecimal digits of the code, and converts them into a 5 digits decimal number, the unique code which identifies the card. In addition, the system converts the 8 previous bits of the data string (b<sub>23</sub>...b<sub>16</sub>), in other words the 2 previous hexadecimal digits of the code, into a 3 digits decimal number which may be used as a 'site code', an identical code for all the cards of the site.

If this site code has not to be checked, leave '0' in the '**Customer code length**' field. If this code has to be checked (and therefore is present in all the cards of the site), select the value '3' in this field and type the 3-digit code in the '**Customer code value**' field.

For example: If the Wiegand hexadecimal code is **12AB08**, the site code is **018** (the decimal value of h12) and the Card code is **00043784** (the decimal value of hAB08).

- **Decimal 24 bits:** In this format, CROW controllers may read up to 50 bits Wiegand string and convert it in two decimal numbers as per the 'Decimal' format but the 3 digit site code is add to the first 5 digits code. The 3 digit Site code may or may not be checked as per the 'Decimal' format.

For example: If the Wiegand hexadecimal code is **12AB08**, the site code is **018** (the decimal value of h12) and the Card code is **01843784** (43784 is the decimal value of hAB08).

### 3.2.2.5. Controller - Readers - Finger Print

This screen configures the biometric readers. ***This tab will NOT be displayed if the reader has NOT been defined as a biometric reader***, in the '[Controller - Reader - General](#)' tab.

Note: Biometric readers received from CROW (from Bioscrypt technology) are pre-configured so they can be directly installed in a system managed by the ProNet application. This configuration is written on the back of each reader and is as follows:

- Type (BioFlex, BioProx, BioPass),
- Address (each manufactured reader has a unique address),
- Default baud rate is set to 38400bps,
- Port mode is set to "2". (I.e., the reader may communicate with the PC either through its Host port RS485, or via its Aux port in RS232).

If the biometric reader is not provided by CROW, the reader must be configured according to the mentioned configuration, through VeriAdmin (Bioscrypt software utility). In this case, once the unit is properly configured, it is important to check that the communication between this software and the reader is correct before using it with ProNet.

### Operating Mode

Each biometric reader is connected to the system via 2 links simultaneously:

- One from its Wiegand OUT to the controller Wiegand IN (in order to send the cardholder code),

- One from its communication port (Host or Aux) to the PC (to receive configuration and templates).

- In the “[Controller Network](#)” screen, define the network on which the biometric reader is connected. Controllers and readers can communicate on the same bus, so this network can be an existing controller network. For TCP network, port **10001** must be used; this means that the TCP/RS485 interface must be configured with the port 10001.

Note: With a **BioPass** reader type, the “[Waiting Delay](#)” parameter of the network must be at least **500** msec.

- In the “[Tools - Options - Communication](#)” screen, select the Bioscrypt readers Baudrate. This baud rate can be different from the controllers baud rate. By default, the baud rate of the CROW biometric readers is **38400 bauds**. This is the default value indicated in the Options screen too.

Note: If the biometric readers network is a TCP type network, the controllers baud rate must be **identical** to the biometric readers baud rate (required to 38400).

- In the ‘[Controller - General](#)’ screen, select the controller on which the biometric reader is connected, click on the ‘Reader’ tab and open the “[Reader](#)” screen of the corresponding reader. In the ‘Technology’ field, choose ‘**Wiegand**’ and in the ‘Biometrics’ field, select the required biometric reader type (the reader type is written at the back of the reader). For **BioFlex** readers with keypad, select the ‘**Wiegand Keypad**’ Technology.


Note: It is recommended to give a reader name that includes the word ‘bio’ (like ‘Bio Rdr1’) to make the identification and future searches easy.

Click on the ‘[Miscellaneous / Badge format](#)’ tab and select the badge format according to the cards in use. For BioPass readers (not using badges) and BioFlex readers with keypad, select the ‘**Decimal**’ Format.

Note: When several readers are defined with the same technology, they must have the same badge format. If some readers need a different format, their technology must be different (i.e. ‘Wiegand 2’) and they must be connected on a different controller.

- Click the ‘[Finger Print](#)’ tab and configure the current biometric reader by specifying the Reader communication network and the reader address (written on the back of the reader). Specify if the reader also serves for enrollment and set the Bio Wiegand format. For BioPass readers and BioFlex readers with keypad, select the ‘**Standard 26 bits**’.

Note: On any given controller, all readers **must** be identical regarding the three following points: Technology, Badge format, Bio Wiegand format.

- Test the communication by opening the “[Diagnose](#)” screen (‘F8’ function key): click on the ‘Biometric readers’ button, on the right top of the screen, then on the  symbol located at the left of the network name and highlight the biometric reader created previously. The communication is established if a **✓** is displayed next to the reader name. Then, on the right window, you can see the memory usage and the reader name with its address.
- In the “[Parameter - All Cardholders - General](#)” screen, create a cardholder and define his access authorization. Click on the ‘Create new’ button for creating a badge. Save.

Note: To each cardholder, the system attributes two codes: the card code and the Bio ID code (or Bio template ID).

- From the “[Parameter - All Cardholders - General](#)” screen of this cardholder, press the ‘[Biometrics data](#)’ button. Select from the list the required enrollment reader and press the ‘Enroll’ button for a fingerprint enrollment. Follow the instructions displayed at the screen. Once the enrollment is finished, an image of the fingerprint template is displayed on the

screen. To save it and to download it to the biometric readers, press 'Save'. After the template data is well received by the readers, the "Save" button is greyed out.

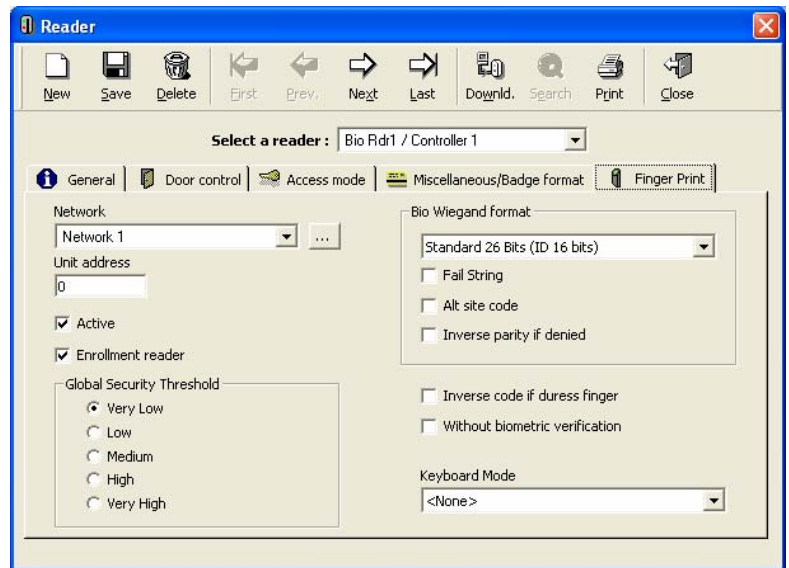
## Fields

**Network:** Select the reader communication network or create a new network by clicking on the [...] button.

**Unit address:** Enter the biometric reader address (written on the back of the reader).

**Active:** Check this box if the reader is physically connected with the network. ProNet communicates only with the active readers.

**Enrollment reader:** Check this box if the reader also serves for enrollment.



Note: A biometric reader can act as an enrolment reader in addition to its normal function as a regular access reader.

**Global security threshold:** This parameter determines the reader security strictness (this option is not visible for BioPass readers).

Note: Since the verification process always uses the lower of the two security levels (the global one and the personal template one), a global setting of 'Very High' means that the verification threshold used will always be the one stored on the template. If the global threshold is set to 'Medium', the threshold used will never exceed medium.

**Bio Wiegand Format:** Select the Wiegand format in which the biometric reader sends the user code to the controller following a successful identification had been achieved. This format must be defined according to the badge format in use (26 bits, etc.). The default format is 'Standard 26 bit'. The three following options apply **only to the standard Bio Wiegand format (not with Custom formats)**:

- **Fail string Code:** Checking this box displays a text box through which the user can define a code that will be sent to the controller following a failed verification (i.e. wrong finger). This code should be a number from 1 to 65535. If this option is not checked then no code will be sent in case of biometric failures.
- **Alt Site code:** This option, when enabled, will cause the unit to replace the real Site Code (normally sent, in addition to the user code, as a part of the Wiegand string upon a successful verification) with the alternate Site Code specified in the edit box.
- **Invert Parity if denied:** Checking this option causes the biometric readers to send to the controllers a special code (card code with inverted parity bits) upon a fingerprint failed verification (i.e. the right badge with the wrong finger): ProNet will therefore be able to display the cardholder name of the rejected transaction. This option (not visible for BioPass readers) is **only available on controllers where the 'Wiegand WITH parity check' option is enable (through the technology dip switches controller selection) with EPROM from 20/07/2004 or later.**

**Inverse code if Duress Finger:** The duress finger mode offers users a way to indicate a duress situation (such as when an employee cardholder is being forced to open a door). In this case the employee should identify himself to the system using a finger predesignated as a "duress finger". Each template can be specified as such by checking the 'Make Duress Finger'



checkbox within the "[Biometrics data](#)" screen of a cardholder. When a successful verification occurs with such a template, the unit will perform the special action specified, such as reversing the Wiegand output to alert the door controller of the duress situation. The controller will grant the access and send to ProNet the event 'Access Granted (Duress Code)'. This option is available **only if the Technology/Badge Format/Bio Wiegand Format is 'Wiegand/Hexadecimal/Standard 26 bits' and when the controllers are set to 'Wiegand WITHOUT parity check' option (through the technology dip switches controller selection) and EPROM from 20/07/2004 or later.**

**Without Biometric Verification:** *This option is visible after pressing Shift and F12 keys.* This option apply with BioFlex or BioProx readers. It allows the user to turn biometric verification off (i.e. no finger required for access) and send the badge code directly to the controller. Turning fingerprint authentication off will result in a less secure system and is not recommended!

USING THIS OPTION DISABLES THE FINGER VERIFICATION AND IS A SECURITY RISK!

**Keyboard Mode:** This option is only visible for BioFlex readers. Select the way to send the user Keypad PIN to the BioFlex reader:

- **Buffered keys in string 26 Bits:** The code as a whole is sent in one string.
- **Key by key:** Each time a key is pressed, its code is sent.

## Tips & Notes

### **'Custom' Bio Wiegand Format**

Each template needs to be downloaded to the biometric readers with an identification number (Called "Bio ID" or "Bio template ID"), which identifies the person. This Bio ID depends on the Bio Wiegand format defined (as the card code depends on the Badge format defined). Normally, the Bio ID is calculated by the system from the last numbers of the card code. For example, the 'Standard 26 bits' Bio Wiegand format calculates the Bio ID from the 4 last digits of the card code.

Nevertheless, the length of this number could be not sufficient in some cases. For example, when 2 badges have the same 4 last digits (561234 and 781234), they will have the same Bio ID. To prevent this risk of duplicates, there are 'Custom' formats which allow to customize the Bio ID computation.

### Examples of Bio Wiegand formats:

- **'Standard 26 bits' format:** The Bio ID is the decimal conversion of the last 4 hexadecimal digits of the card code. This format allows also the 'Inverse parity' and 'Duress code' features
- **'Standard 37 bits' format:** The Bio ID is the decimal conversion of the last 6 hexadecimal digits of the card code. This format allows also the 'Inverse parity' and 'Duress code' features.
- **'Custom Pass-Thru' format:** A customized Bio format which allows the user to define which bits to use in the Wiegand bits string to define the Bio ID. This format get three parameters:
  - Total bits:** Bits total number of the Wiegand card code read by the reader.
  - ID Start bit:** First bit position of the Bio ID among the card code.
  - ID Length bits:** Bits total number which compose the Bio ID.
- **'Custom 6 digits' format:** The Bio ID is the decimal conversion of all the 6 hexadecimal digits which compose the 26 bits card code.
  - Total bits = **26**
  - ID Start bit = **1**
  - ID Length bits = **24**

Note: The calculation method used by the application to compute the Bio ID from the card code depends on: (1) the Badge Format and (2) the Bio Wiegand Format.

If the Badge format and the Bio Wiegand format are the same for all the controllers and all the biometric readers, the algorithm which links the card code and the Bio ID is the same for all the system and therefore the cardholders Bio ID are similar on all the biometric readers. The templates and their Bio ID numbers may be broadcasted to all the biometric readers.

Therefore, in a normal situation, it is recommended to have the same format definitions throughout the whole system.

### **3.3.3. Controller - Input**

The informative table summarizes the input parameters connected to the controllers. Default parameters are defined according to the controller type. To obtain more detailed information and modify input data click on the [...] **button** situated to the right of the table of the corresponding tab.

Inputs are used for access control or for alarm monitoring purposes:

- **Access control:**
  - **Door control:** A door contact device is connected to an input: the two input states open or closed correspond to the two door status: open or close. An alarm is activated in case a door is forced or left open beyond the specified 'door alarm delay' period
  - **Exit request:** A RTX button ('Request to Exit') is connected to the input: pushing this button will lead to the activation of the corresponding door relay
- **Alarm monitoring:**
  - **General alarm input:** A sensor/detector (magnetic contacts, movement detectors, etc.) is connected to an input: the two input states open or closed correspond to the two possible status of the detector: normal or under alarm.

The 'normally' state (either 'normally open' or 'normally closed') of an input is the status, open or closed, into which the input is not under alarm.

When an armed input goes under its alarm status, it triggers:



An alarm at the central station  
 Predefined relays or local reflexes  
 Automatic processes or predefined global reflexes

## Table analysis

**Num:** Number of the selected

**Name:** Name of the input

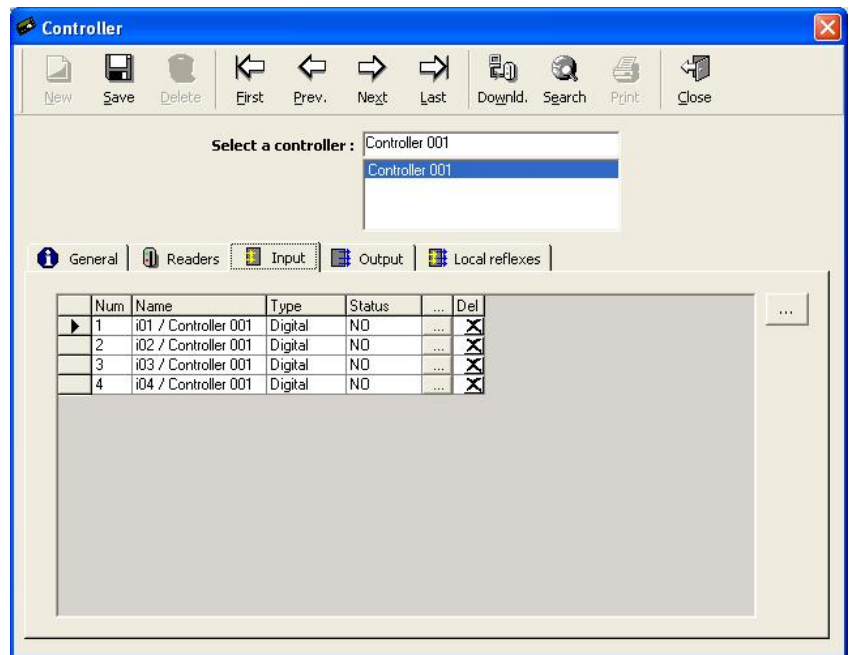
**Type:** Mention if the input type is Digital, Digital 4 states or Analog.

**Status:** Input normal status, i.e. normally open (NO), normally closed (NC) or State 1 to 4.

**Button [...]** (on the input line): Click on this button to display the “[Input](#)” screen for creating, consulting or modifying data

**Button [x]** (on the input line): Click on this button to remove the input from the list displayed

**Button [...]** (outside the table): Click on this button to display the “[Input](#)” screen even if no input is selected



### 3.3.3.1. Controller - Input - General Screen

The “Input” screen enables the input parameter definition. It can be reached from to the corresponding tab of the “Parameter - Controller” screen, by clicking on the [...] button situated to the right of the table.

## Fields

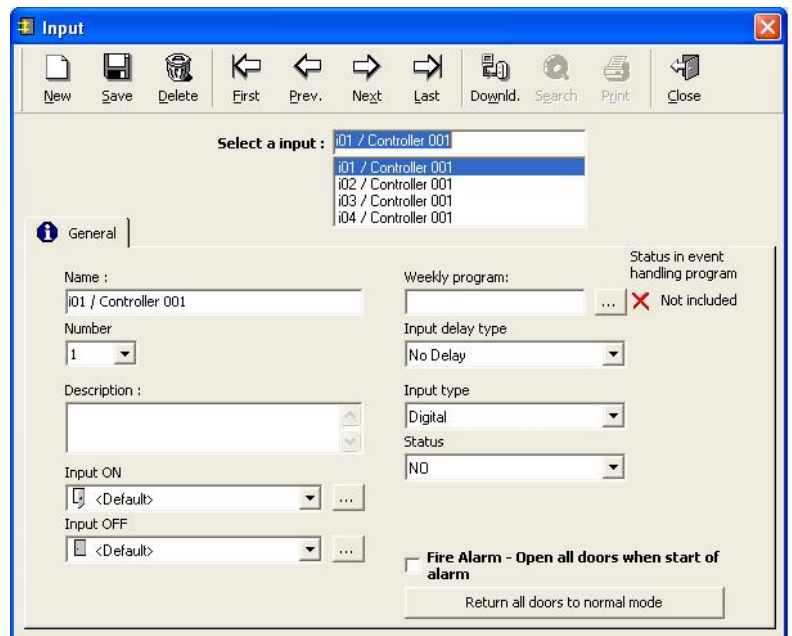
**Name:** Name the input

**Number:** Choose the input number; the maximum input number connectable depends on the type of controller used (See ‘[Types of controllers and associated readers, inputs and outputs](#)’ in the “Controller – General” Chapter)

**Description:** Describe the new data entry

**Input ON:** Select the icon that graphically represents the input in its physically ‘ON’ position in the maps or click on the [...] button for creating a new one.

**Input OFF:** Select the icon that graphically represents the input in its physically ‘OFF’ position in the maps or click on the [...] button for creating a new one.



### Input delay type:

- **No delay:** An alarm is raised as soon as the input is activated
- **After... (if on alarm):** Specify the number of seconds beyond which an alarm is raised if the input is still activated
- **After... (even if no more on alarm):** Specify the number of seconds beyond which an alarm is raised, even if the input is not activated

### Input type:

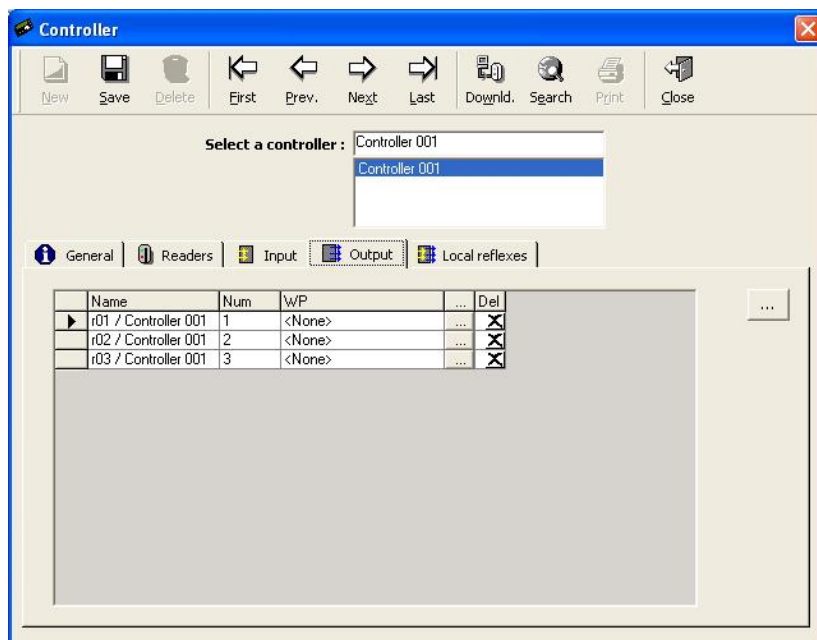
- **Digital** (2 states): The input may have two states only: open or closed, which correspond to the two possible states of the sensor/detector connected to the input.
- **Digital 4 states:** In addition to the two basic states of the sensor/detector (open or closed), the input may detect two supplementary states which correspond to the status of the line used to connect the sensor/detector to the input: line cut or line short.
- **Analog:** The input can take different decimal values according to the sensor connected to it (temperature, etc.) and triggers alarms or specific action when it reaches pre-defined values (by default, three limit values are defined: 2 / 2.88 / 4).

Consult the controller documentation to check which type of inputs is available in the controller.

**Status:** Choose the status among: NO, normally open or NC, normally closed or State 1 to 4, in which the input is NOT under alarm.

### 3.3.4. Controller - Output

The informative table summarizes the parameters of the controllers outputs. An output is materialized by a relay located on the controller board (or on its extension board) to which an external device may be connected and therefore activated by the controller. (Door opener, siren, etc.) Default relays numbers are defined according to controller definition. To obtain more detailed information and modify input data, click on the [...] button situated to the right of the table of the corresponding tab.



### Table analysis

**Name:** Name of the output

**Num:** Number of the output selected

**WP:** Name of the weekly program associated to the output, defining the activation and non-activation periods

**Latest action:** Mention of the last action that could have affected the output; for instance, the action that closed a “normally open” output by a global reflex

**Button [...]** (on the relay line): Click on this button to display the “[Output](#)” screen for creating, consulting or modifying data

**Button [x]** (on the relay line): Click on this button to delete the output from the list displayed

**Button [...]** (outside the table): Click on this button to display the “[Output](#)” screen even if no item is selected

### 3.3.4.1. Controller - Output - General Screen

The “Output” screen allows output parameter definition. It is accessible by going to the corresponding tab of the “Parameter - Controller” screen and clicking on the [...] button located to the right of the table.

#### Fields

**Name:** Name the output

**Description:** Describe the new data entry

**Number:** Choose the output number; the maximum number depends on the type of controller used (See '[Types of controllers and associated readers, inputs and outputs](#)' in the “Controller – General” Chapter)

**Weekly program:** When a Weekly program is selected, the relays will be automatically activated during the ‘green periods’ defined by this program (and deactivated during the ‘red periods’ of the program). Click on the [...] button to create or modify the weekly program.

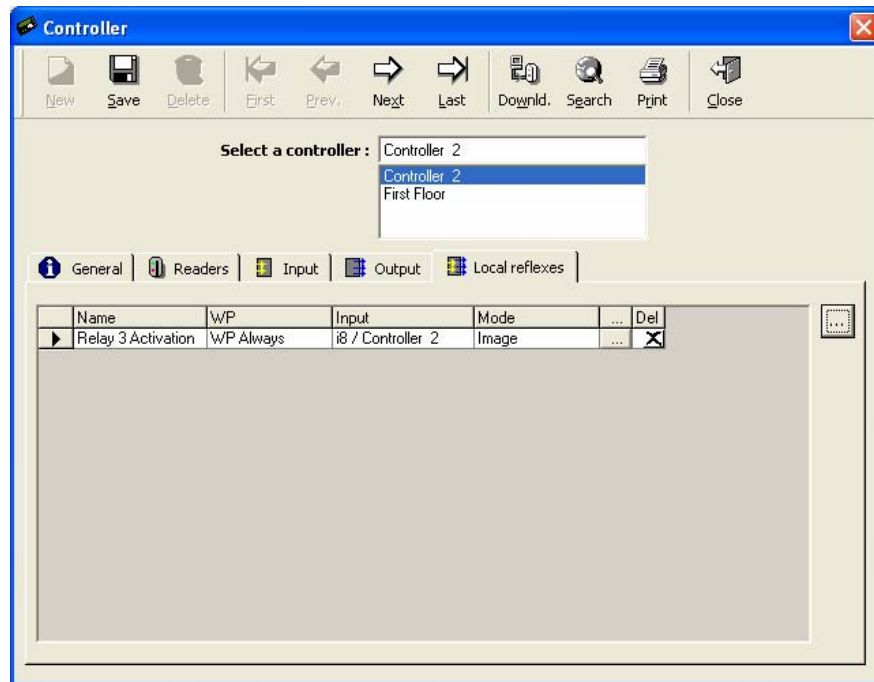
Note: Do not allocate weekly program to door relays. Time activation of door relays has to be set from the '[Controller – Reader – Door control](#)' screen. Allocating weekly program through this ‘Output’ screen may result in a definition conflict.

**Latest action:** Mention the last action that could have affected the output; for instance, the action that closed a “normally open” output by a global reflex.

### 3.3.5. Controller - Local Reflexes

A local reflex defines the outputs activation following the trigger of an input of this same controller. The reflex occurs even if communication with the controller is interrupted. The “[Local reflex](#)” screen defines the link between the inputs and the outputs.

The informative table summarizes the parameters of the local reflexes associated to the controller. To obtain more detailed information and modify the data, click on the [...] button situated to the right of the table of the corresponding tab.



#### Table analysis

**Name:** Name of the reflex

**WP:** The local reflex weekly program defines the reflex activation and non-activation periods

**Input:** Name of the input that sets off the local reflex

**Mode:** Type of action set off by the local reflex (Image, Constant ON, During)

**Button [...]** (on the line of the reflex): Click on this button to display the “[Local reflex](#)” screen, in order to consult or modify data

**Button [X]** (on the line of the reflex): Click on this button to delete the reflex from the list displayed

**Button [...]** (outside the table): Click on this button to display the “[Local reflex](#)” screen, even if no item is selected

### 3.3.5.1. Controller - Local reflex - General Screen

A local reflex defines the outputs activation following the trigger of an input of this same controller.

The “Local reflex” screen allows the definition of the reflex parameters. It is accessible by going to the corresponding tab of the “Parameter - Controller” screen and clicking on the [...] button located to the right of the table.

#### Fields

**Name:** Name the reflex

**Weekly program:** Choose from the list the weekly program which defines the reflex activation and non-activation periods or click on the [...] button to create or modify the weekly program

**Description:** Describe the new data entry

**Input:** From the list, choose the input setting off the local reflex or click on the [...] button to create a new input

**Input status:** Select the status of the input which sets off the local reflex: Start of alarm, End of alarm, Line short, Line cut, Open, Close, <Any Status>.

**Outputs:** Click on the  or  buttons, to declare which relays to activate or to deactivate

**Action type:** Choose the type of action set off by the local reflex:

- **Image:** When the input is activated, the reflex is activated and when the input is deactivated, the reflex is deactivated at the same time
- **Constant ON:** When the input is activated, the reflex is activated and stays activated, even if the input is deactivated
- **During:** When the input is activated, the reflex is activated during a predefined delay (to define from 1 – 120 sec.).

Note: Alternated mode (During = 122 Sec): The reflex is activated after the input is activated and stays activated; the reflex is only deactivated after a second input activation and stays deactivated, and so on.

## 3.4. Time Zone

### 3.4.1. Basic Concepts

Time zones consist of calendar divisions into daily, weekly and holiday time segments associated to predetermined system functions.

The system recognizes:

- **Daily program:** division of a 24-hour day into access zones ('green' time periods) and non-access zones ('red' time periods)
- **Weekly program:** made up of a daily program for each day of the week and a supplementary daily program for holidays
- **Holiday:** dates specified as holidays

During the 'green' periods of a Daily Program, the system behaves as follows:

- **Cardholders** may access different areas of a site according to their access group
- **Readers** operate in predefined the access mode recorded as 'Security Level 1'
- **Alarms** are armed
- **Relays** are automatically activated

#### Time zone application table

|                | Within the limits of the Time Zones<br>(‘Green’ periods) | Beyond the limits of the Time Zones<br>(‘Red’ periods) |
|----------------|--|--|
| Access control | Access granted according to<br>access group              | Access denied  |
| Readers        | Access mode Security Level 1                             | Access mode Security Level 2                           |
| Alarm zones    | Armed  | Not armed  |
| Relays         | Activated  | Non activated  |

#### Tips & Notes

##### Arming alarms

Refer to the "[Event Handling Program - Alarm](#)" paragraph for more information regarding how to arm an alarm.

##### Importance of a proper definition

Properly defining time zones is essential for the system to work optimally. It is highly recommended to successively specify the daily, weekly and holiday programs prior to defining the other parameters of the system.

##### Maximum number of usable programs

Many daily, weekly and holiday programs can be created in the whole the system but each controller may include a restricted number of usable programs (99 Daily Programs, 32 Access Weekly Programs, 80 Event Weekly Programs and 60 holidays). An error message appears if the limit of usable programs has been exceeded for a specific controller.

### 3.4.2. Daily Program

The division of days (24H) into time zones, to which are associated the system predetermined functions, is defined in this screen. A Daily Program divides a 24H day in 2 time zones which therefore defines 5 time periods, 3 'Red' and 2 'Green'.

Note that it is possible to divide each day into 4 times zones and therefore create 5 'red' and 4 'green' periods. (by changing the option '2 times zones' to '4 time zones' in the field 'Daily Program Time zones' on the '[Tools – Options – Communication](#)' screen)

The screenshot shows the 'Daily program' window with the 'General' tab selected. The 'Name' field contains 'Working Day' and the 'Company' dropdown is set to 'Building Manager'. The 'Description' field is empty. Under 'Time zone 1', the start time is 08:00 and the end time is 12:00. Under 'Time zone 2', the start time is 14:00 and the end time is 18:00. At the bottom, a horizontal ruler shows the 24-hour day from 0 to 23:59. The ruler is divided into segments: red from 08:00 to 12:00, green from 12:00 to 14:00, red from 14:00 to 18:00, green from 18:00 to 20:00, and red from 20:00 to 23:59.

#### Fields

**Name:** Name the new daily program; examples: part-time AM, night team

**Company:** Company the item refers to (for use with multi-company application ONLY).

**Description:** Describe the new data entry

**Time zones 1 - 2** (or 1 - 4): Define the limits of the 2 (or 4) time zones using the format XX:YY, where X = hour and Y = minute

**The ruler at the bottom of the screen** gives the time frames in a visual manner.

- The **green** frames represent the 'Green periods' (4 maximum)
- The **red** frames represent the 'Red periods' (5 maximum)

#### Tips & Notes

##### **Programs by default**

The two daily programs "Always" and "Never" are defined by default. Their denomination can be modified but the two programs can neither be erased or their contents modified.

##### **New daily program**

By default, the time frames for a new daily program are from 8 AM to 12 AM and from 2 PM to 6 PM.



### 3.4.3. Weekly Program

A weekly program is made up of 8 daily programs, one for each day of the week and an extra program for holidays. Two more daily programs can be added (in the "[Tools - Options - General](#)" screen) for having other access control in some days in the year (i.e. the day before a National day, annually closure or exceptional opening, etc.). This last feature requires the use of controllers equipped with an EPROM from 01/06/2004 or later.

| Time Slot   | Program     | Day |
|-------------|-------------|-----|
| 00:00-00:00 | Never       | Su  |
| 08:00-12:00 | Working Day | Mo  |
| 14:00-18:00 | Working Day | Tu  |
| 08:00-12:00 | Working Day | We  |
| 14:00-18:00 | Working Day | Th  |
| 08:00-12:00 | Working Day | Fr  |
| 14:00-18:00 | Working Day | Sa  |
| 00:00-00:00 | Never       | Hd  |
| 00:00-00:00 | Never       | S1  |
| 00:00-23:59 | Always      | S2  |
| 00:00-00:00 | Never       | S2  |

#### Fields

**Name:** Name the new weekly program

**Company:** Company the item refers to (for use with multi-company application ONLY).

**Description:** Describe the new data entry

**Daily programs:** One for each day of the week (Su - Sa), one for holidays (Hd) and if needed, one for each special day (S1 – S2); select the adequate program from the list or create a new daily program by clicking on the corresponding button associated to the day

**Time frames** corresponding to the program selected are displayed on a grey background.

#### Tips & Notes

##### **Programs by default**

The two weekly programs "WP Always" and "WP Never" are defined by default. Their denomination can be modified but both programs can neither be deleted nor modified.

##### **Deactivating Holiday and Special Days**

Holiday and special days daily programs can be defined as <usual daily program of the day> in order to deactivate the rule of these specific days, for some employees if needed.

### 3.4.4. Holiday

Days considered holidays by the system are defined in this screen. During these holidays, Daily Program in use (and therefore system behaviour) is the 8<sup>th</sup> program defined in the Weekly Program (or the 9<sup>th</sup> or the 10<sup>th</sup> program in case of using special days; see the previous paragraph).

#### Fields

**Name:** Name the new holiday

**Description:** Describe the new data entry

**Company:** Company the item refers to (for use with multi-company application ONLY).

**Single Day & Many Days:** Select if the new data concerns one single day or a several days period.

**From:** The current date is listed by default. In the calendar, it will appear circled in red. To call up the calendar, click on the arrow situated to the right of the current date. Select the day, month and year in the calendar that appears on the screen or enter directly the date.

On the calendar, by clicking on "Today" the actual date is selected.

#### To select a given month

- Produce the list of months by pressing on the name of the month displayed
- Skip from one month to the next by pressing on one of the double arrow keys ends (next to the month)
- Scroll the calendar from month to month by pressing and maintaining depressed on one of the double arrow keys ends (next to the month)

#### To select the desired year

- By clicking on the displayed year appear double arrow keys (next to the year). Skip from one year to the next by pressing on one of the double arrow keys
- Scroll the calendar from year to year by pressing and maintaining depressed on one of the double arrow keys ends (next to the year)

**To:** If the holidays last several days, select the 'Many days' option and enter here the last day.

**Each year:** Select to repeat the definition of a holiday for coming years; for example, Christmas always falls on the 25th of December.

**Day type:** Select the holiday type (Holiday, Special Day 1 or Special Day 2).

### 3.5. Access Group

This function determines “who can go where and when”. The access group attributed to employees determines the doors accessible, the weekly programs associated to the doors and the door crisis level.

To use this function:

- Select the authorized doors for the individuals of a group
- Associate the corresponding weekly programs
- Attribute a crisis level to each access group, door by door
- Attribute an access group to each employee, in the “[Parameter - All Cardholders - General](#)” screen

| Reader ...             | Weekly program ... |
|------------------------|--------------------|
| Rdr01 / Controller 001 | w/P Never          |
| Rdr02 / Controller 001 | w/P Always         |

#### Fields

**Name:** Enter a name for the access group

**Description:** Describe the new data entry

**View:**

- Check **V** button to display readers list for which access is granted for the selected group
- Check **X** button to display readers list for which access is refused for the selected group

**First column of the table:** **V** or **X**

- Select **V** to include the reader in the access group
- Select **X** to exclude the reader from the access group

**Reader:** List of readers and doors associated

**Weekly program:** Select the weekly programs associated to the reader from the list

## Tips & Notes

### Access group by default

An access group “Anytime Anywhere” is defined by default. It guarantees permanent free access to all doors. Its denomination can be modified but this group can neither be deleted nor modified.

### Minimal authorization by default

When a new data is created, status for all doors is checked. By default, minimal authorization is granted.

### Many access groups

The system does not limit the number of access groups. However if a large number of access groups are required due to the variability of the badge holders’ work hours, it is recommended:

- To create an access group that guarantees permanent free access at authorized doors, with the weekly program: <Use Personal WP> and the crisis level: <Use personal crisis level>
- To restrict access by using personal weekly programs and individual crisis levels, in the personalized data of the badge holder.

### Different error message

Please note the difference in the error message associated to an access refusal in the following two cases:

|   | Reader ...          | Weekly Program ... | Error message if access denied: |
|---|---------------------|--------------------|---------------------------------|
| ✓ | Rdr1 / Controller 1 | WP Never           | “Not authorized at this time”   |
| ✗ | Rdr1 / Controller 1 | WP Always          | “Reader not allowed”            |

## 3.6. Department

A department is a functional notion, which allows site division into various work areas. This function is mostly informative. A department can be chosen as a selection criterion to display and print reports.

### Examples

Administration, Top Management

### Fields

**Name:** Name the new department

**Description:** Describe the new data entry

The screenshot shows a window titled "Department" with a standard toolbar (New, Save, Delete, First, Prev., Next, Last, Download, Search, Print, Close). Below the toolbar, there is a "Select a department:" label followed by a list box containing "Purchasing Dept", "Purchasing Dept", "R & D", "Sales Dept", and "Top Management". Below this, there is a tabbed interface with a "General" tab selected. The "General" tab contains two fields: "Name:" with the value "Purchasing Dept" and "Description:" with an empty text area.

### 3.7. Badge

This screen defines the badges used and displays their owners.

#### Fields

**Create a group of badges:** Click for creating a series of badges (in another new window, see [Group of Badges](#) paragraph).

**Advanced settings:** Displays advanced features related to biometric readers.

**Code:** Enter directly the card code. Generally, this code is written on the badge as a sequence of 8 characters using numbers from “0” to “9” and letters from “A” to “F”. If the length of the code is shorter than 8 characters the system will complement it by adding zeros at the beginning of the code. A default badge code can be automatically inserted at the beginning of all badge codes with the “[Tools -Options - General](#)” screen.

**Note:** This code is downloaded to the controllers and saved in the application database. The code may be read differently according to the reading technology defined in the “[Reader - General](#)” tab and the Badge format defined through the ‘[Reader - Miscellaneous/Badge format](#)’ tab.

**Get from card:** Click for opening the following screen in order to get the code by reading the card:

- To get the card code from a regular reader, pass the card on one of these readers: when the card code appears on the window, select it and press OK.
- To get the card code from a biometric reader, select the relevant reader in the lower ‘get card code from bio reader’ window, press the button right to this list and pass the card to the selected reader: when the card code appears on the window, select it and press OK.

| Card Code | Reader              | Date             |
|-----------|---------------------|------------------|
| 009B477C  | Rdr2 / Controller 2 | 03/11/2005 15:41 |
| 009B4780  | Rdr2 / Controller 2 | 03/11/2005 15:41 |
| 00698299  | Rdr1 / Controller 2 | 03/11/2005 15:41 |

**Type:** Select the badge technology from the displayed list (Magnetic, Wiegand, etc.).

**Note:** Reading technology is defined in the ‘Technology’ field in the “[Parameter - Controller - Reader - General](#)” screen. Only badges data compatible with the selected technology will be downloaded to the readers.

**Status:** Specify the badge status: **Used**, **Cancelled**, **Free** (default), **Lost**, **Stolen**. A badge cancelled, lost or stolen is automatically invalidated by the system.

**Bio template ID:** Each template needs to be downloaded to the biometric readers with an identification number (Bio ID or Bio template ID), which identifies the person. This number, displayed and editable in this field, is automatically computed by the system from the card code (see the "[‘Custom’ Bio Wiegand Format](#)" paragraph), based on the Badge format (defined through the "[Reader - Miscellaneous/Badge format](#)" tab) and the Bio Wiegand format (defined in the "[Reader - Finger Print](#)" tab).

**Note:** Make sure that the system has calculated the Bio ID and that is not 0. Cards that were defined prior to the creation of the first biometric reader, will have Bio ID = 0. For these cards, calculation of the corresponding Bio Template ID will be done automatically only when the card owners will enroll the finger. After a biometric reader definition, each new badge will receive automatically a Bio ID code, which is displayed in the 'Bio template ID' field after saving. A manual calculating is also possible by selecting the "**Advance settings**" box and pressing '**Calculate 1**' (to re-calculate the selected badge) or '**Calculate all**' (for all badges in the database, including those that are not 0). If the field remains empty or null it means that the system cannot calculate the Bio ID and it has to be entered manually or be read directly from the biometric reader. To obtain the code from the card itself, use the 'Get Bio ID' window field. There you need to select the reader from the list, click on the 'ID' button, and pass the badge at the biometric reader.

**Owner:** Select to assign a badge to an employee; when an attributed code is selected, the name and surname of the badge holder appear in this field. The field remains empty if the code entered is not attributed. Click on the [...] button to display the [employee's](#) screen.

**Description:** Describe the new data entry

**Get Bio ID:** *Visible by checking the 'Advanced settings' box.* To enroll directly the Bio ID from a biometric reader (BioProx or BioFlex), select the relevant enrollment reader from the list, click on the '**ID**' button and then pass the badge at the selected biometric reader. The Bio ID should appear on the 'Bio template ID' field.

## Tips & Notes

### **Recording Bio ID with BioPass and BioFlex + Keypad**

When only BioPass or BioFlex with keypad readers are used in the system, cards are not requested. However, a badge (even if it does not physically exist) must be attributed to each person. Therefore, the 'Technology/Badge format' of these readers must be 'Wiegand/Decimal' (even if no cards are used) and the Bio Wiegand format must be 'Standard 26 bits'. Card codes may be manually entered through the 'Code' field or using the 'Create a group of badges' function. The system then may calculate the Bio ID which is, in this case, equal to the card code. The PIN code to use at the keypad connected to the BioFlex will be this Bio ID, which is a **maximum 5 digits code (max. 65535)**.

### **Card code or badge format change**

After changing a card code, a re-calculation of the Bio ID is needed for that card only ('Calculate 1' button). However, in a case of modification of the 'Badge format' or the 'Bio Wiegand Format', a re-calculation of the Bio ID for all card ('Calculate ALL' button) is needed plus initialization of all the Biometric readers (from the "[Diagnose](#)" screen).



### 3.7.1. Badge Search

#### Displaying the list of all the attributed badges

Double click on the “Search” icon of the icon bar.

#### Performing a search on a specific type, status or owner

To find a badge from its type, status or owner:

- Click on the “Search” icon of the icon bar (or type “F10” key)
- Select the desired type, status or owner
- Click on the “Search” icon a second time
  - If the badge is attributed, details of the badge will be displayed on the screen
  - If no badge has been found, the fields remain empty and the screen has a grey shade
- Click on the “Search” icon to display the list of all the attributed badges

#### Searching a badge from all or part of its code

When pressing on the “Search” icon, if the first characters of the code have been entered, the system will display all the badges that start with the desired sequence, after pressing on the “Search” icon a second time.

#### Examples:

| In the “Code” field type | The system displays all the card codes attributed                                     |
|--------------------------|---|
| 32                       | Beginning with “32”   |
| 32%45                    | Beginning with “32”, which contain the characters “45”                                |
| _ _ _ _ 32 _ _           | Which contain the characters "32" at the 5 <sup>th</sup> and 6 <sup>th</sup> position |

#### Note:

% will replace several characters

\_ (underscore) will replace one single character

### 3.7.2. Group of Badges

This screen allows the creation and deletion of a group of badges in a single command. It is accessible via the [“Parameter - Badge”](#) or [“Tools - Create a group of badges”](#) menu.

#### 3.7.2.1. Group of Badges - Create

Create a group of badges in a single command using this tab.

#### Fields

**First card code:** Type the 8-character code assigned to the first badge

Note: A beginning card code common to all badges can be set in the [“Tools - Options - General”](#) screen.

**Quantity:** Type or select the number of badges to create; the list has been provided for information. The maximum number of badges depends on the plug limitation.

**Type:** Choose the badge technology from the displayed list (Magnetic, Wiegand, etc.).

Note: The choice of reading technology will enable selective data download to the readers. Only data compatible with the selected technology will be downloaded to the readers.

**Position to increment** (between 0 and 8): Define the position of the character to increment in the 8-character sequence making up the code. This allows keeping a constant group of characters as code endings. ***To use this function, it is necessary that only decimal numbers compose the beginning of the code, till the position to increment.***

#### Example

| First card code | Position to increment |
|-----------------|-----------------------|
| 12345ABC        | 5                     |

The next code:

12346ABC

**Create also cardholders:** Create simultaneously a group of badges and their associated badge holders, which will have:

- **Basic parameters:** Valid employee parameters to whom the “Anytime Anywhere” access group is attributed
- **Set parameters same as:** Specify the name of the badge holder whose parameters will serve as reference for the new badges

### 3.7.2.2. Group of Badges - Remove

Remove a group of badges in a single command using this tab.

The screenshot shows a dialog box titled "Create a group of badges" with a blue header bar and a close button (X) in the top right corner. Inside the dialog, there are two tabs: "Create" and "Remove". The "Remove" tab is selected and highlighted. Below the tabs, there are three input fields: "First card code" (a text box), "Quantity" (a dropdown menu showing "1"), and "Position to increment" (a dropdown menu showing "8"). To the right of the "First card code" field is a "Remove" button, and to the right of the "Quantity" field is a "Cancel" button. Below these fields is a checkbox labeled "Remove also cardholders" which is currently unchecked. At the bottom of the dialog, there are two buttons: "Remove all non allocated badges" and "Remove all deleted cardholders".

#### Fields

**First card code:** Type the 8-character code assigned to the first badge

**Quantity:** Type or select the number of badges to delete; the list has been provided for information. The maximum number of badges depends on the controller and plug limitation.

**Position to increment** (between 0 and 8): Define the position of the character to increment in the 8-character sequence making up the code. This allows keeping a constant group of characters as code endings. ***To use this function, it is necessary that only decimal numbers compose the beginning of the code, till the position to increment.***

#### Example

| First card code | Position to increment |
|-----------------|-----------------------|
| 12345ABC        | 5                     |

The next code:

12346ABC

**Remove also cardholders:** Delete simultaneously a group of badges and their corresponding badge holders

**Remove all non allocated badges:** Delete all cards that are not allocated anymore, i.e. temporary cards

**Remove all deleted cardholders:** Select to remove all deleted cardholders from the database

## 3.8. All cardholders

### 3.8.1. All cardholders - Basic Concepts

Each badge holder, employee, visitor or guard, that requires access authorization to the site must be recorded beforehand in the database. To access or modify information related only to visitor or guard, consult the screens "[Parameters - Visitor](#)" or "[Guard Module](#)".

The "Parameter - All cardholders" screen defines the details of all the users, employee and visitor alike.

#### Tips & Notes

#### Quick definition

The family name is the only obligatory field for creating a new badge. Nevertheless, in order to grant access, the field "Badge" is necessary. The "Anytime Anywhere" access group is associated by default to the new cardholder.

### 3.8.2. All cardholders - General

This screen records general information about the badge holder.

The screenshot shows the 'Cardholder' application window with a blue title bar and a standard Windows-style toolbar. The main area is divided into several sections:

- Toolbar:** Contains icons for New, Save, Delete, First, Prev., Next, Last, Download, Search, Print, and Close.
- Select a cardholder:** A dropdown menu showing 'Johnson Linda - 8234'.
- Display photo:** A checkbox that is checked, with a 'Show deleted' link below it.
- General Tab:** Contains fields for:
  - Last name: Johnson
  - First name: Linda
  - Number: 8234
  - Type: Employee (dropdown)
  - Company: IFSECX
  - Location: Department (Sales Dept. dropdown), Office phone (568125793)
  - Badge: 01234573
  - Access: Access group (Day team dropdown), PIN code (\*\*\*\*), Personal weekly program (WP Always dropdown)
  - From date: 15/07/2007 16:56
  - To date: 15/07/2007 16:56
  - Validated: checked
- Photo:** A small portrait photo of a woman is displayed on the right side of the General tab.
- Buttons:** Create new, Allocate, Edit, Remove, and Biometrics data.

## Fields

**Display photo:** Check this box to display the employee's picture

**Show deleted:** Check this box to display the deleted badge holders; by default, this box is unchecked

Click on the **Delete button** (in the tool bar) to delete the badge holder from the database. Deleted badge holders are not erased from the database but saved under the type "Deleted". They are not displayed by default.

Actions following the badge holder deletion:

- The badge holder is classified as "Deleted"
- The corresponding badge allocation is removed
- The badge is added to the non-allocated badges list
- The validation case is unchecked
- The record disappears from the badge holder screen, unless the "Show deleted" box is checked

Note: Only allocated cards are taken into account into the computation of the plug limitation.

**Last name & First name:** Type the last name and the first name of the cardholder. It is possible to create cardholders with the same last and first name. In this case, it is necessary to enter a unique number per person in the "Number" field and to check the "Allow duplicate name of cardholders" option in the "[Tools – Options - General](#)".

**Number:** Enter an identification number

**Type:** Choose the cardholder type (Employee, Visitor or Guard); the "Type" field does not appear in the "[Parameters - Visitor](#)" or "[Guard Module](#)" screens

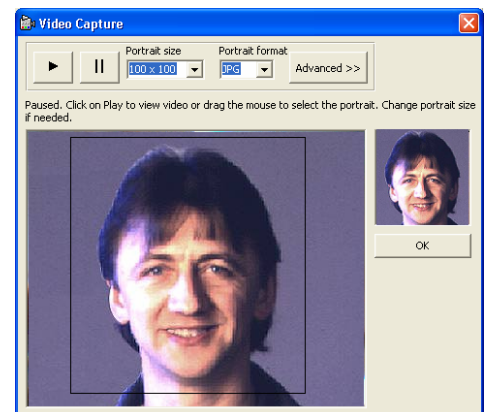
**Company:** Mention the name of the company the badge holder works for

**Employee's picture:** Click on the following button

- **Select a picture:** To select the name of the file beholding the employee's picture (jpeg or bmp format)
- **Remove picture:** To remove the employee's picture
- **Take a snapshot:** To open the following "Video Capture" screen:

Users which have a camera video or a web cam can play and pause the live video stream, select the required image size, and then move the mouse over the paused image to select the part of the image they wish to keep as the cardholder image.

- **Print a badge or define badge printing layouts:** To open the screen of badge printing layouts (Refer to the "[All cardholders - Badge Printing Module](#)" paragraph for more information).



**Location:**

**Department:** Select the department the employee works for from the list provided or create a new department by clicking on the [...] button

**Office phone:** Mention the office phone number, the cell phone number, etc.

**Badge:**

- **Create new:** Create a new badge and associate it to an employee (in "[Badge](#)" screen)
- **Allocate:** Allocate an existing badge
- **Edit:** Display details of the badge in use (i.e. for modification)
- **Remove:** Remove the badge allocation

Note: A cardholder cannot have several badges of the same technology.

- **Biometrics data:** Create, modify or delete the employee's fingerprint templates (Refer to the "[All cardholders - Biometrics data](#)" paragraph for more information).

**Access:**

**Access group:** Select an access group from the list or click on the [...] button

**Personal weekly program:** Select the personal weekly program from the list or create a new program by clicking on the [...] button; this program is only used if the access group of the selected cardholder has been predefined with the <Use Personal WP> weekly program

**PIN code:** Mention the badge holder personal identification code to enter on the reader keypad; this code is common to all the reading technologies used

**Personal crisis level:** Select the individual crisis level, between 0 and 7; this crisis level is only used if the access group of the selected cardholder has been predefined with the <Use personal crisis level> crisis level

**From date:** Specify the beginning date of the validation period of the badge holder. Type data in directly or select a date by using the direction arrows.

**To date:** Specify the date and hour when the badge validity will end. Type data in directly or select a date by using the direction arrows.

**Validated:** Check this box to validate badge use; a non-validated badge exists in the database but its use will be forbidden

To define a validation period

- Uncheck (clear) the "Validation" box
- Check the "From Date" box and / or check the "To Date" box
- Set the validation period in date in the "From Date" and / or "To Date" fields
- Save

Note: If the validation date chosen belongs to the past, the "Validation" box will be checked automatically. Beyond the specified validity date, the badge will automatically become invalid. Every 30 minutes, at xx:15 and xx:45, the program checks if new cardholders need validating or invalidating, in which case the corresponding cardholders definitions are sent to the controllers. The frequency of this checking may be modified through the '[Tools - Options - Communication](#)' screen (default: 30 minutes).

**Set as default:** By checking this box, the badge holder selected serves as a reference. His parameters are automatically copied as default parameters for newly created badge holders. This function saves the trouble of having to define the same parameters for each cardholder that will be created in the future.



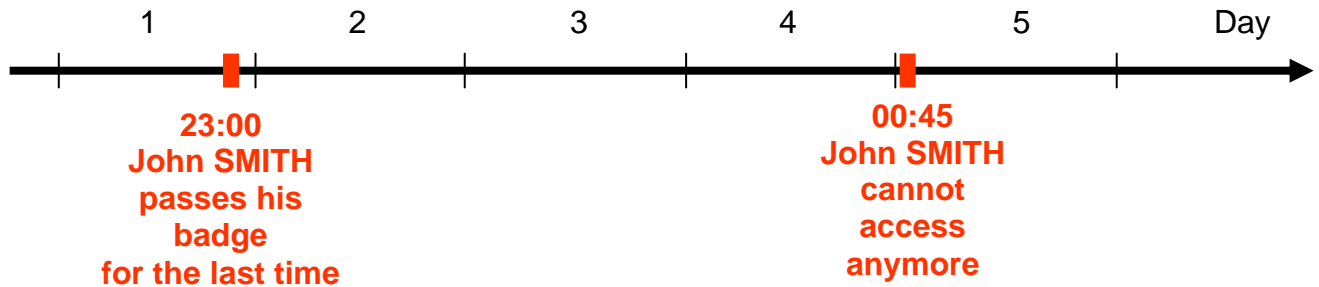
## Tips & Notes

### Automatic card inhibition if a card not used after X days

It is possible to inhibit automatically cardholders who have not used their card during X days. The checking is done each night at 00:45.

#### Example:

Let us take a system configured to inhibit all the cardholders that did not pass their badge during 3 days.



A cardholder that passed his badge the day '1' (at any hour!) will have access on days '2', '3' and '4'. If he did not pass his badge at a reader of the system during these 3 days, the system will invalidate automatically his badge on day '5' at 00:45 a.m.

#### Operating Mode :

- Exit the application and look for the ini file at the main application folder.
- Open it with Notepad and look for the following entry:

```
AutomaticInhibition = 0
```

*If this line does not exist, run the application, go to "Tools - Options" and click "OK". This operation rebuilds the ini file and inserts all the possible entries according to the latest application version.*

- Set the value according to the required days number before inhibition.

Example, to inhibit all the cardholders that did not pass their badge during 3 days, set:

```
AutomaticInhibition = 3
```

- Save and close this file, and restart ProNet.

#### Note :

If the PC is turned off all the nights, the inhibition command will not be able to be sent to the readers at 00:45 a.m. This function works only if **the application is running at that time.**

### ➤ 3.8.4. All cardholders - Biometrics data

This screen allows creating, modifying and deleting cardholder fingerprint templates directly from the “[All cardholders - General](#)” screen, through the ‘Biometrics data’ button.

#### Operating Mode

Once a biometric reader is configured for use as an ‘Enrollment reader’, it is possible to enroll fingerprints for existing users. The information created during the enrollment process is stored as a ‘Template’. Template contains one fingerprint, its associated card code and other related data. Each template is save twice: in the ProNet database, as well as in all the active biometric readers.

- In the current screen, select the relevant biometric reader from the combo list (This list displays only readers defined as ‘Enrollment readers’).
- Press the ‘Enroll’ button for fingerprint enrollment, then follow the instructions on the screen. The message “PLACE your finger on the sensor” should appear.
- Put the finger on the reader until the graphical image of the fingerprint appears on the screen and the message changes to “Remove finger. Ready to save”.
- Press the ‘Save’ button for saving this fingerprint and for downloading it to all the active biometric readers.

#### Fields

**Select an enrollment reader:** from the active enrollment biometric readers drop-down list.

#### **Step 1: Enroll your fingerprint:**

**Enroll:** Click to enroll a fingerprint or to re-enroll an existing fingerprint.

**New:** Add supplementary templates for same cardholder. In each new template a different finger can be enrolled or a previous existing finger. Enrolling an existing finger twice, enhances the chance that fingerprint will be recognized by the biometric unit.

**Delete:** Delete the template from the database and remove it from the biometric readers. A progress bar in the bottom of the screen will give an indication of the delete process.

#### **Fingerprint picture:**

- **Quality:** Template quality score. The minimum satisfying score is **50** (3 blue stars).
- **Content:** Template content score. The minimum satisfying score is **70** (4 blue stars).

The screenshot shows the 'Biometric Data' window. At the top, there's a dropdown menu for 'Select an enrolment reader:' with 'Rdr1 bio/ Controller 1' selected. Below this is a 'Fingerprint' tab. The main area is divided into two sections: 'Step 1: Enroll your fingerprint' and 'Step 2: Accept the template'. In Step 1, there's an 'Enroll' button and a 'New' button. A fingerprint image is shown on the left. To the right of the image, there are two rows of stars: 'QUALITY' with 54 points (3 blue stars and 1 half star) and 'CONTENT' with 97 points (4 blue stars). In Step 2, there's a 'Finger' section with a diagram of a hand and a '1:1 Security Threshold' section with radio buttons for 'Very Low', 'Low', 'Medium' (selected), 'High', 'Very High', and 'None'. At the bottom, there are buttons for 'Download Template', 'Save', and 'Exit', along with a progress bar showing '1 / 1'.

## Step 2: Accept the template:

**Finger:** Indicate which hand finger has been enrolled.

- **Make duress finger:** Check this box if this finger is only use in duress situation.

**Security Threshold:** Threshold related to the quality and content of the fingerprint information.

Note: The 'None' threshold may be selected, enabling, for instance, the director's fingerprint to be accepted even with a failed verification. (Note however, that such setting creates a security risk in case the director's card was stolen).

**Download Template:** Click to download the current template to all the biometric readers of the system. A progress bar in the bottom of the screen will indicate the status of the download.

**Buttons [ |◀][◀] [▶][▶| ]:** Browse between the different templates of the cardholder.

**Save:** Click for saving the current template and for downloading it to all the biometric readers.

**Exit:** Click for close this screen.

## Tips & Notes

### Suggested Fingers type

It is recommended to use index, middle or ring fingers. Avoid using thumb and pinky fingers since they are typically awkward to consistently position on the sensor.

### Finger Placement

By putting the finger on the reader, cover completely the entire area of the sensor with the fingerprint for providing the best performance. Touching the sensor as if pressing a button creates an image that lacks information-rich fingerprint data.

### Deleting Cardholder Templates

When a cardholder is deleted, all his templates regardless of the card serial number are removed from the biometric readers and deleted from the database.

### Managing Badges

If a cardholder loses his badge and wishes to receive a new badge without the need to re-enroll his entire fingerprints, follow these steps:

- In the "[All cardholders](#)" screen, select the relevant cardholder from the combo list.
- Press the 'Edit' button to open the "[Badge](#)" screen.
- In the 'Code' field enter the code of the new badge, and save the record.
- Select the 'Advanced setting' checkbox and press the 'Calculate 1' button. This will re-calculate the Bio ID according to the new card code.
- Save and exit this screen and return to the "All cardholders" screen.
- Click '[Biometric data](#)' and press 'Download template': the application will then remove the old templates and download the same templates but with the new Bio template ID.

### Downloading Interruption

In case of temporary communication failure during the templates download process, the action will be stored as a pending command. Later, when communication is regained, the pending commands will be executed.

### 3.9. Visitor

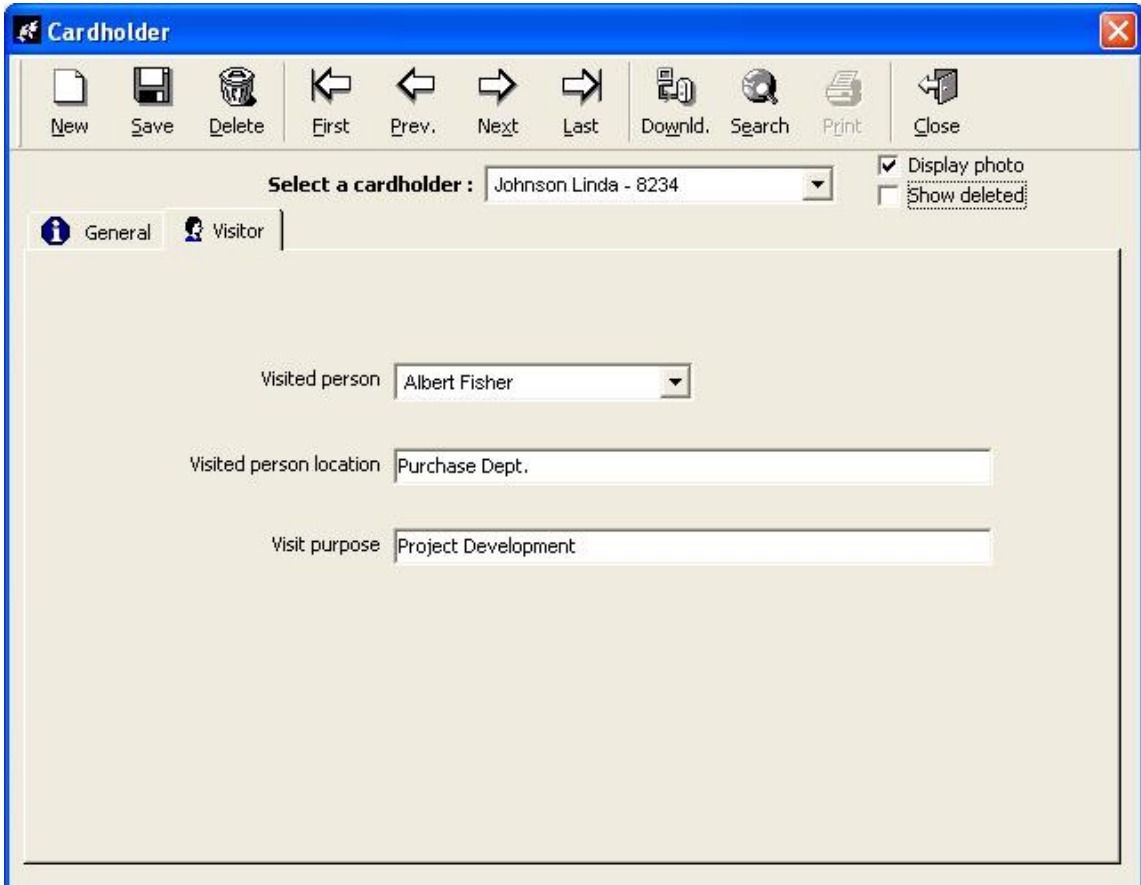
The system distinguishes occasional visitors from employees. The “Parameter - Visitor” screen allows consulting and modifying information with respect to visitors only.

#### Example

This enables the secretary at the entrance of the building, or the guard, to create a temporary badge for visitors without having the need to access the main employees database.

Note: This screen is identical to the “[Parameter - All Cardholders](#)” screen except that the “Type” field is set to visitor and does not appear on the screen.

When a cardholder is defined as “Visitor”, the new tab “Visitor” is added, to specify visit information.



The screenshot shows a software window titled "Cardholder" with a standard menu bar (New, Save, Delete, First, Prev., Next, Last, Downld., Search, Print, Close). Below the menu bar, there is a "Select a cardholder:" dropdown menu currently showing "Johnson Linda - 8234". To the right of this menu are two checkboxes: "Display photo" (checked) and "Show deleted" (unchecked). Below these are two tabs: "General" and "Visitor", with the "Visitor" tab being the active one. The "Visitor" tab contains three input fields: "Visited person" with a dropdown menu showing "Albert Fisher", "Visited person location" with a text box containing "Purchase Dept.", and "Visit purpose" with a text box containing "Project Development".

#### Fields

**Visited person:** Select in the list of cardholders

**Visited person location:** Specify the requested information

**Visit purpose:** Specify the requested information

### 3.10. Authorization Levels

An authorization level is a group of options and screens which can be viewed and/or modified by users who belong to the level.

#### Examples



- The site manager has access to all the information
- The parking lot attendant can only modify information regarding parking and view user details
- The secretary at the entrance of the building can only create visitors' badges

Once authorization levels have been created (through the following screen), they must be attributed to users in the "[Parameter - User](#)" screen.

#### Fields

**Name:** Name the new authorization level

data entry

**View:** Determine the authorization level for each option and menu. The  symbol indicates a head of chapter. In order to produce the sub-menus click on the symbol  located to the left of the name of the menu.

**Screen status:** **V** or **X** or **R**

The application allows differentiating within a head chapter, the screens that are accessible, restricted and forbidden. Viewing status can be modified by clicking successively on the sign to the left of the screen definition:

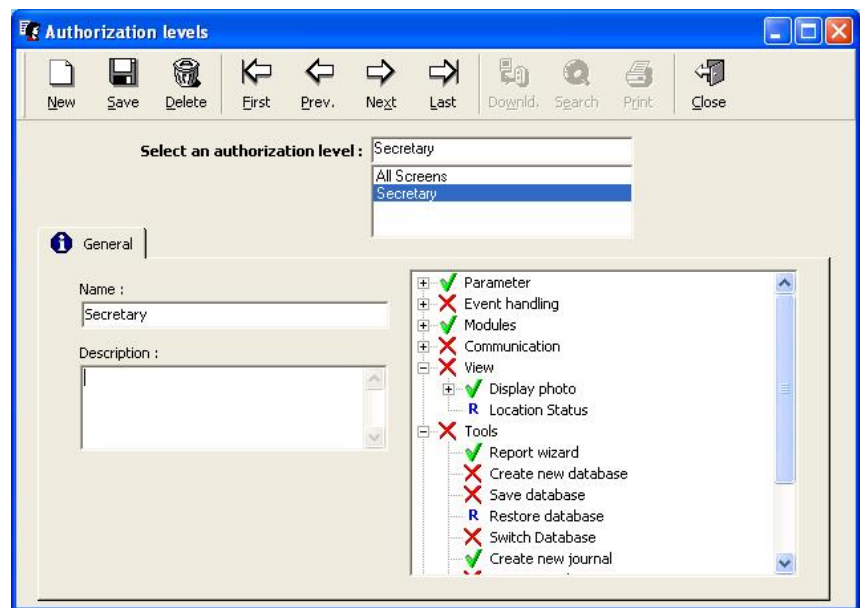
- Select **V**, to define accessible screen (read, write and delete)
- Select **X**, to define forbidden screen
- Select **R**, to define restricted screen (read only, without modification)

By changing the status of the head chapter, it applies automatically the same status to all sub-menus that it contains. For example, if access to a head chapter is **X** to a group of users, access to all sub-menus will automatically be **X**. But, the status of sub-menus can be changed individually.

#### Tips & Notes

##### Authorization level by default

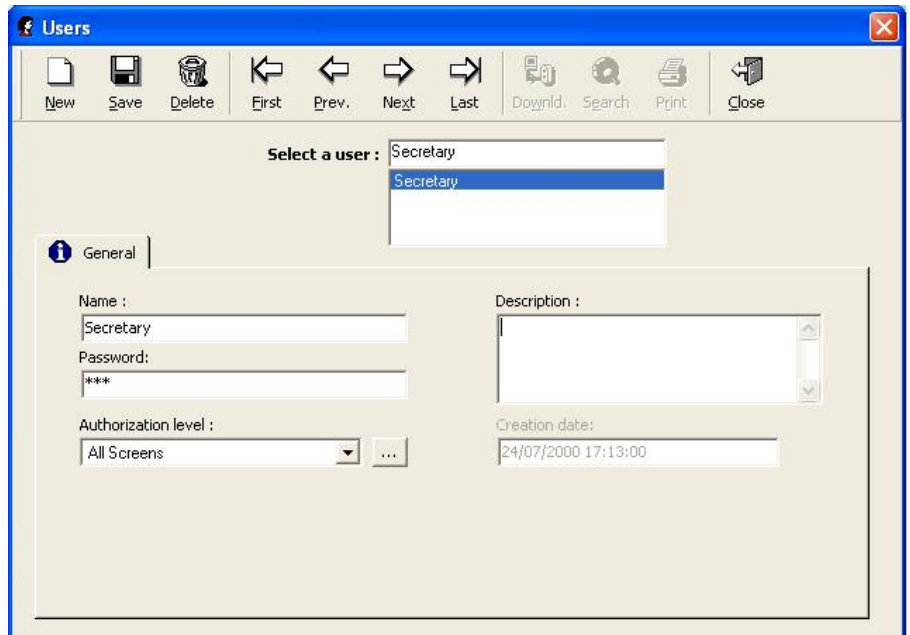
By default, an authorization level – "All screens" – is defined. It corresponds to a maximum accessibility (all options and screens are accessible). Its denomination can be modified but this level can neither be deleted nor modified.



### 3.11. User

An User is a person who can access the ProNet application. Creation of users with attribution of authorization level and password are allowed in this screen.

In order to limit authorization levels within the system, it is advised to define the authorization levels before creating user data.



The screenshot shows a window titled "Users" with a standard Windows-style toolbar at the top containing icons for New, Save, Delete, First, Prev., Next, Last, Download, Search, Print, and Close. Below the toolbar, there is a "Select a user :" dropdown menu with "Secretary" selected. The main area is divided into a "General" tab. Within this tab, there are several input fields: "Name :" with "Secretary" entered, "Password:" with "\*\*\*" entered, "Authorization level :" with a dropdown menu showing "All Screens" and a button "...", "Description :" with a large empty text area, and "Creation date:" with a date/time field showing "24/07/2000 17:13:00".

#### Fields

**Name:** Name the new user

**Password:** Type the password that the user will use to enter the system

**Authorization level:** Select an authorization level from the existing list or click on the [...] button to create another authorization level

**Company** (only visible by Super user): Mentions the company the item refers to or click on the [...] button to create another company (for use with multi-company application ONLY).

**Super user** (only visible by Super user): Special user whose functions are the creation of new companies, the allocation of first users within each entities and the decision of who the other super-users will be (for use with multi-company application ONLY).

**Description:** Describe the new data entry

**Creation date:** Displayed automatically by the system without possibility of modification

#### Tips & Notes

##### **See the password**

Double click on the password to make it appear on the screen.



### 3.12. Log Off

The "Log Off" function allows different users to log in and off the system. After log off, the "Login" screen is displayed. Only authorized user, with adequate user name and password, can access the ProNet system.


This can be used to prevent system access to unauthorized users, while the program is running.

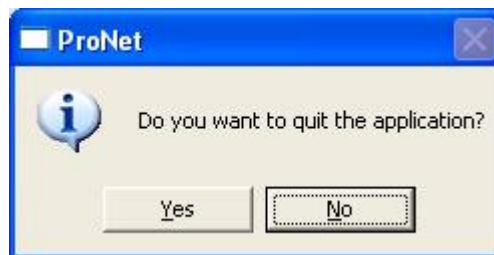
An automatic log off can be set in the system. The log off delay can be modified or cancelled in the "[Tools - Options - General](#)" screen. If selected, it is set by default to 10 minutes.



### 3.13. Exiting the Application

In order to terminate a work session and exit the application, choose one of the following steps:

- Click on the "Exit" icon represented by a door, at the far right of the navigation bar
- Double-click on the icon represented by a magical wand, in the upper left corner of the screen
- Click on the cross , in the upper right corner of the screen
- Click on the "F4" function key and, at the same time, on the "Alt" key
- Open the "Parameter" menu and choose the "Exit" option (at the bottom of the list)



## 4. “Event handling” MENU

The “Event Handling” section of the application manages alarms, presents them graphically on maps, creates actions and processes and combines them in global reflexes following certain events.

### Icons, maps and position

The graphical functions of the ProNet software integrate the dynamic display of inputs on installation maps.

- Define icons (“[Event-Handling - Icon](#)” screen), certain icons are defined by default
- Link the icons to the inputs (“[Parameter - Controller - Input](#)” screen)
- Define site maps (“[Event-Handling - Maps](#)” screen)
- Position the inputs on the maps (“[Event-Handling - Position](#)” screen)
- Display the final status in the “[Event-Handling – Active alarms](#)” screen

### Operating Mode of the “Event Handling” menu

- Define the inputs
- Gather the inputs into an input group (if necessary)
- Define the outputs
- Gather the outputs in an output group (if necessary)
- Define the action to set off, following an input or group of inputs activation
- Define the process, in other words, the sequence of actions
- Define the global reflex, in other words, the events that generates the reflex and the actions to trigger

### 4.1. Icon

Icons are graphical symbols, attributed to input, output, map, process or action. They will be positioned on maps and will be used dynamically in the “[Event-handling – Active Alarms](#)” screen.

Icons of controllers’ inputs and outputs are created by default.

Basic graphical symbols are supplied in the directory:

“C:\Program Files\ProNet5\Media\Icons”

Other icons can be added by specifying their name, description and location on the disc. They are automatically stored with all the icons in the directory mentioned above.

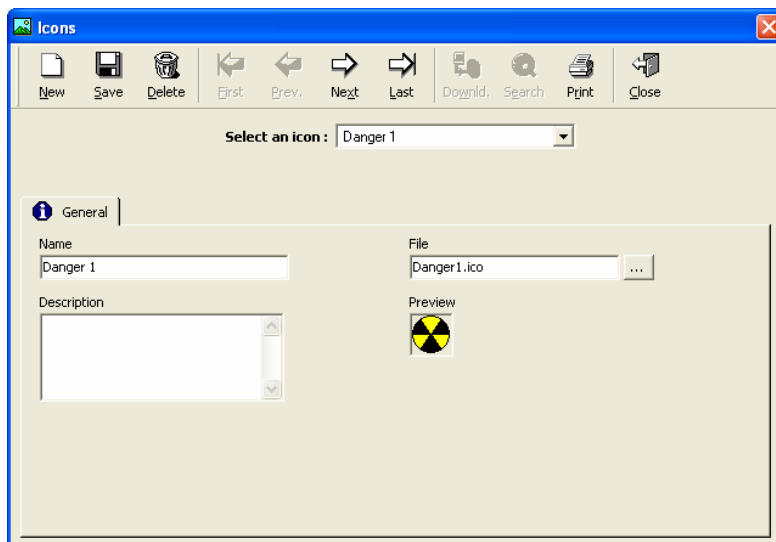
### Fields

**Name:** Type the icon name

**Description:** Describe the new data entry

**File:** Select the name of the file beholding the associated graphical symbol; click on the [...] button to chose another file and specify its address.

**Preview:** Display the image of the selected icon



## 4.2. Map

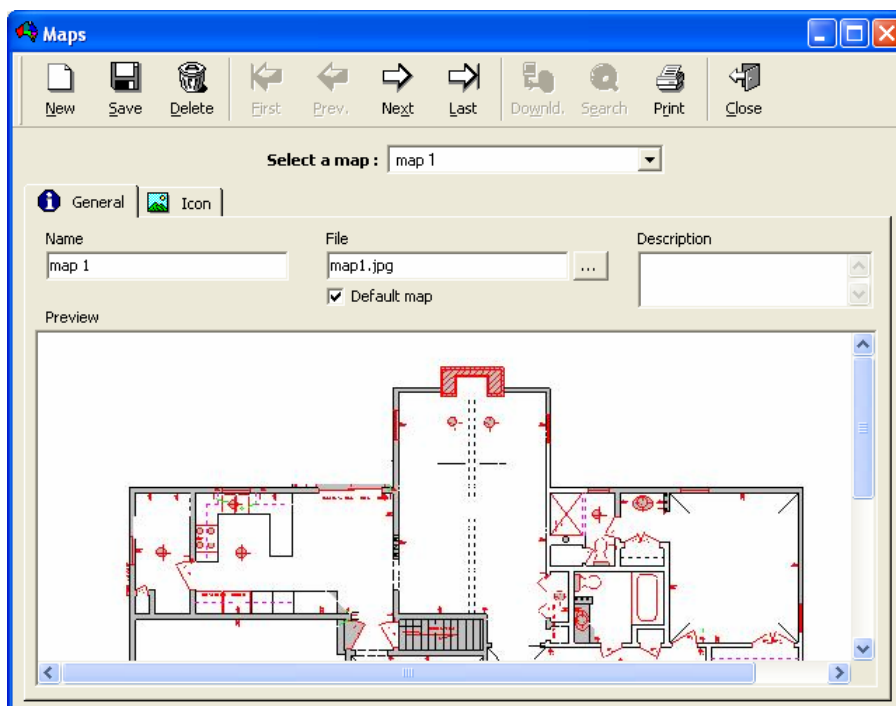
The “Maps” screen allows the integration of maps into the software. In order to use the “[Active Alarms](#)” function, inputs must be positioned on maps.

It is advised to store all maps in the following directory:

“C:\Program Files\ProNet5\Media\Maps”

### 4.2.1. Map - General

A cascade of maps can be defined. For instance, the maps representing the different floors can be linked to the map of a multi-floor building.



#### Fields

**Name:** Type the name of the map

**File:** Display the name of the file beholding the map; click on the [...] button to choose another file and to specify its address.

**Description:** Describe the new data entry

**Default map:** Check the box for setting the selected map as default map; it will be displayed automatically on opening the “[Active Alarms](#)” screen.

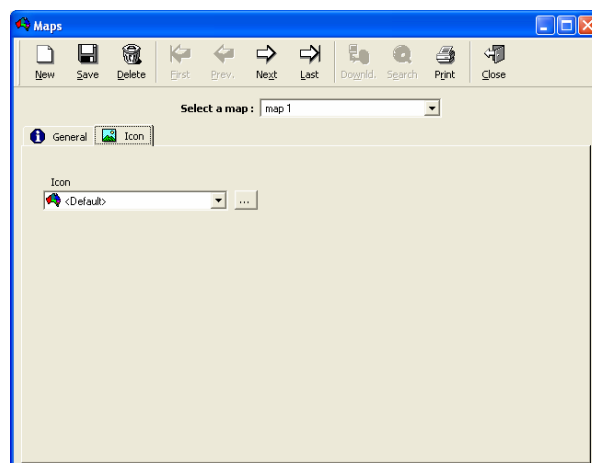
**Preview:** Display the map selected

### 4.2.2. Map - Icon

This screen enables the association of icons to maps.

#### Field

**Icon:** Select the icon to associate to the map from the list, or select the [...] button to create a new one.

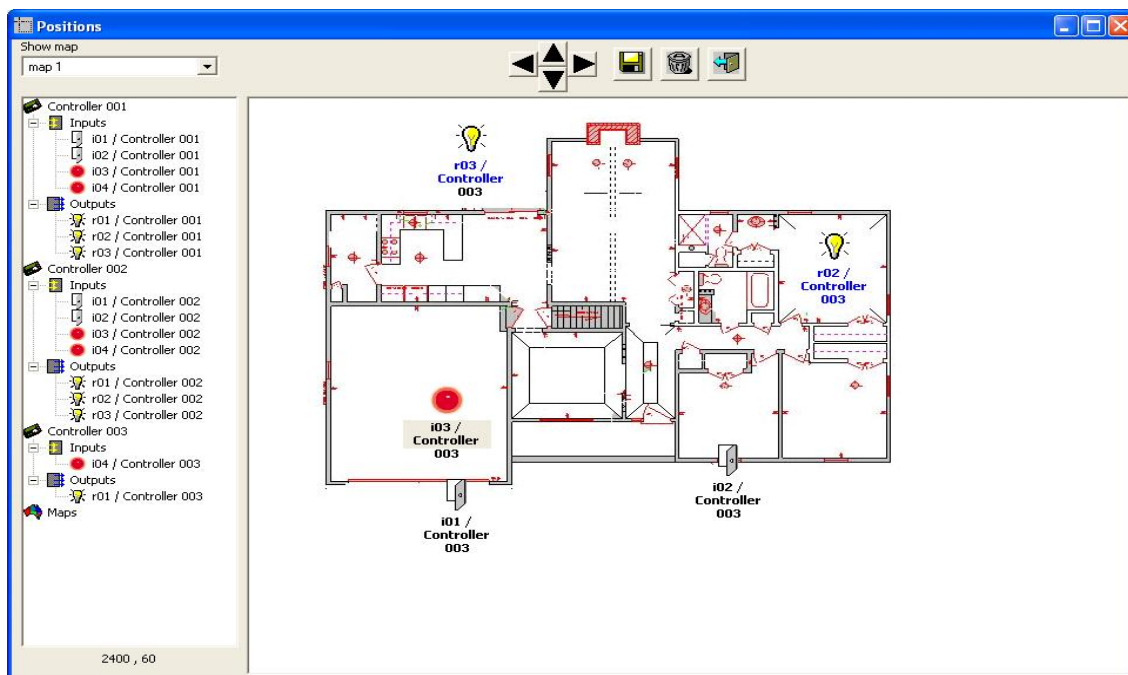


### 4.3. Position

The “Position” option allows the positioning of inputs, outputs, maps, processes and actions on the maps.

In the left window are listed active controllers, inputs, outputs, maps, process and actions.

Drag the icon from the left column and drop it into the map, then save the positioning. Fine-tune the placing with the arrows. Once positioned, the item will disappear from the list, indeed each icon can only be positioned once on one map. The icons will be used in the “[Event-Handling - Active Alarms](#)” screen.



### Fields

**Show map:** Choose the map to be displayed from the list

**Left Window:**

- Controllers list with inputs and relays
- Maps list
- Processes list
- Actions list

**Buttons [◀], [▲], [▼] & [▶]:** Click on the four direction arrows to refine the selected icon positioning on the map with accuracy.

**Button [💾]:** Click to save the selected icon positioning

**Button [🗑️]:** Click to remove the selected icon from the map and place it in the list again

**“Exit” Button** (at the far right): Click to exit from the “Position” screen.

### Tips & Notes

#### Positioning

Modifying the input position on the map can be done using a mouse: select the object, maintain the left mouse button depressed and move the mouse towards the new position.

## 4.4. Active Alarms

The Active alarms screen graphically presents inputs, relays and alarms status on a site map. Actions and processes can be triggered by clicking on icons and it is possible to skip from one map to the next.

### 4.4.1. Active Alarms - Basic Concepts

Hereunder some concepts used in this manual:

#### ➤ Inputs concepts:

**Digital Input or Alarm input:** a controller input point to which a sensor/detector (magnetic contacts, movement detectors, door contact device to reflect the door position, etc...) is connected. In general, controllers have by default 4 or 8 inputs and may be extended to 16 or more. The two input status open or closed correspond to the two possible physical status of such sensor/detector: open or close.

**4 states or supervised input:** in addition to the two basic states of the sensor/detector (open or closed), the input may detect two supplementary states which correspond to the status of the line used to connect the sensor/detector to the input: line cut or line short. Note that the alarm linked to this two supplementary status, line cut or short, is always armed, i.e. it is not possible to attribute to them a weekly program. The input type ('digital' or 'digital 4 states') must be indicated in the [input definition screen](#).

Consult the controller documentation to check which type of inputs is available in the controller and how to connect a 4 states input.

**Input status or input physical status:** the physical status of the sensor/detector connected to the input: either open or close.

**Input normal status:** The 'normally' status of an input, either 'NO' for 'Normally Open' or 'NC' for 'Normally Closed', is the status, open or close, into which the sensor/detector connected to this input is *not* under alarm. This normal status must be indicated in the input definition screen (see '[Controller - Input](#)' paragraph).

**Input off/on or input logical status:** An input is 'off' when it is in its normal status and 'on' when it is not in its normal status. It represents the logical status of the input. From the [Input definition screen](#), two icons may be defined (and positioned on a map, as described in the '[Position](#)' paragraph) to represent the logical status of the input, either 'on' or 'off'.

**Armed/disarmed input:** To each input may be attributed a Weekly Program (from the [Input definition screen](#)): the input is 'armed' during the green periods defined in the Weekly Program and 'disarmed' during the red periods (See '[Time zone](#)' chapter for details).

**Activated input:** an input is activated when the following conditions are true: it is armed and its status is 'on', i.e. it is under alarm during green periods of its Weekly program.

### Table of the different Digital Input Status

| Input | Physical status | Normal status | Logical status | WP Activation | Alarme status |
|-------|-----------------|---------------|----------------|---------------|---------------|
| i1    | Open            | NO            | Off            | Armed         |               |
| i2    | Close           | NO            | On             | Armed         | Activated     |
| i3    | Close           | NC            | Off            | Disarmed      |               |
| i4    | Open            | NC            | On             | Disarmed      |               |

#### ➤ Outputs concepts:

**Output:** a controller output point which is in fact the output contact of a controller relay. In general, controllers have by default 4 relays and may be extended to 16 or more. Such relay gives a dry contact, and may be represented by an electrical switch which can be either open or close. When the relay is closed, the device (door, siren, etc.) which is connected to the relay is activated.

**Output status:** the status of the relay, i.e. open (or activated or 'on') or close (or deactivated or 'off'). As for an input, two icons may be defined to represent the output status. (in the [Output definition screen](#))

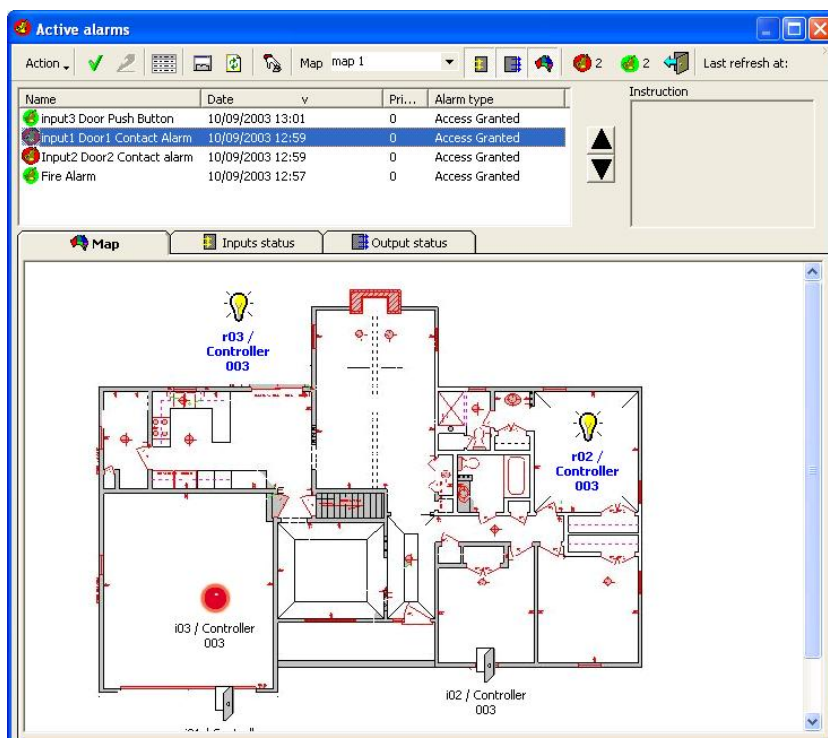
The Active alarms screen is accessible from the Main menu tool bar. It is divided into three tabs:

- [Map](#) tab: allows to display the site maps,
- [Input status](#) tab: allows to display the different status of the inputs,
- [Output status](#) tab: allows to display the different status of the outputs.

#### 4.4.2. Active Alarms - Map

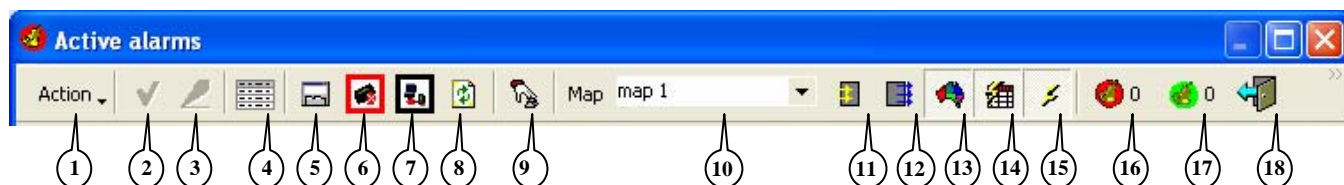
This screen graphically presents the Input/Output status and alarms on a site map per name, date, priority and alarm type.

Only items (inputs, outputs, maps, actions or processes), which have an icon, positioned on the map may be displayed. How to set the icons in the map is described in the chapter "[Position](#)". Actions and processes can be triggered from the same screen by a right click on an icon. It is possible to skip from map to map.





## Toolbar



The functions available from the toolbar are as follows:

- 1: Action menu:** allows more useful actions like Execute a process, Confirm all alarms, etc.
- 2: Acknowledge the alarm:** Select an alarm from the table and acknowledge it; this allows the differentiation between new and already acknowledged alarms. It is advisable to use this function to facilitate alarm management. When an alarm is acknowledged, the following events take place in the table of the “Event Handling - Active Alarms” screen as well as on the navigation bar:
  - The alarm icon goes from red to green
  - The count of acknowledged and non-acknowledged alarms are updated
- 3: Confirm the alarm:** confirm a specific alarm, already acknowledged; a new screen appears displaying the following information:
  - Name
  - Event date and hour
  - Alarm type: start of alarm, line cut or line short.
  - Comment: type in an optional comment, such as importance, user name, etc. the comment will appear in the journal “data” column
- Confirm all** (from the ‘Action’ menu only): confirm *all* the displayed alarms using a single command. This option is useful in case of prolonged communication failure. The computer will ask for confirmation. Individual alarm acknowledgement and confirmation are not required.
- 4: Auto select last alarm / remain on selected alarm:** to conserve or not the focus on the last occurred alarm.
- 5: Show / hide the active alarm table:** to maximize the map on the screen
- 6: Communication error indication:** appears when ProNet does not succeed to communicate with one controller.
- 7: Polling off indication:** appears when the polling has been manually stopped (from the [‘communication’](#) menu)
- 8: Refresh:** manual refresh when there is no polling or when the polling exists but the “Auto-refresh of Input/Output status” is not requested in the [“Tools - Options - Server”](#) screen
- 9: Open the [“Execute Process”](#) screen**
- 10: Map selection list:** Choose the map to display in the list
- 11: Show all inputs:** Press to show all inputs / only active alarms.
- 12: Show outputs:** Press to show / to hide relays.
- 13: Show maps:** Press to show / to hide maps.
- 14: Show processes:** Press to show / to hide processes.
- 15: Show actions:** Press to show / to hide actions
- 16: Number of active alarms:** as well as in the tool bar of the main screen
- 17: Number of acknowledged alarms:** as well as in the tool bar of the main screen
- 18: Exit**

## Data displayed

**Alarm Table:** The window below the toolbar shows the actual alarms status (active, acknowledged or confirmed):

**Name:** Name of the alarm input. The icon before the name shows the alarm status:

- Active (red icon)
- Acknowledged (green icon)
- Confirmed (the alarm disappear)

**Date:** Date and time of the alarm

**Priority:** Alarm priority (defined in the "[Event-Handling Program - Alarm Properties](#)" screen)

**Alarm type:** Start of alarm, line cut or line short

**Buttons [▲] & [▼]:** Click on the direction arrows to select the requested alarm

**Instruction:** Instruction which appears when the alarm is raised (defined in the "[Event-Handling Program - Alarm Properties](#)" screen).

**On the site map:** Point the mouse on an icon in the map, click on the right button and choose among the following functions:

### **Input icons**

- Acknowledge (when under alarm)
- Confirm (when under alarm)
- Open input properties
- Return to normal mode
- Input deactivation

### **Relay icons**

- Open relays properties
- Return to normal mode
- Deactivate relay continuously (constant off)
- Activate relay continuously (constant on)
- Activate relay during, specify the number of seconds

### **Process icons**

- Execute process
- Open process properties

### **Action icons**

- Execute action
- Open action properties

Note: Only the actions allowed for the user will appear.

## Tips & Notes

### **Automatic refresh**

The icons status can be automatically updated by selecting the “Auto-refresh Input/Output status” option in the “[Tools - Options - Server](#)” screen. Alternatively, when the Auto Refresh is off, a manual refresh button can be used on the top bar.

### **Dynamic map management**

In case of several maps, the displayed map is the one encompassing the activated inputs. If no alarm is signalled, the default map is displayed. If several alarms are activated, the map containing the most recent alarm raised will be displayed. If the “Event Handling - Active Alarms” screen is already open and a new alarm belonging to the displayed map is triggered, this map is dynamically updated. Actions and process can be directly executed by right clicking on their icons. It is possible to swap from map to map by selecting the required map either using the map selection drop down menu or by clicking on the appropriate icons, if such icon has been previously positioned.

### **How Alarms are shown**

- If the ‘show all inputs’ button is not selected, the screen shows only the logical status of activated inputs, i.e. the armed inputs actually ‘on’ (active alarms). The icon appears immediately when the alarm is detected, without the need of using the ‘refresh’ button. The icon of an activated input stays in the map until the operator acknowledges and confirms it.
- If the ‘show all inputs’ button is selected, the screen shows the logical status of all the inputs defined in the “[Position](#)” screen.

The dynamic swap of icons allows for visual follow-up of input and output status: activation or deactivation of alarm points, door open or close and relays supervision.

Example: If a door alarm is detected, an icon will show an open door. If the door is closed, the icon will be updated to a closed door.

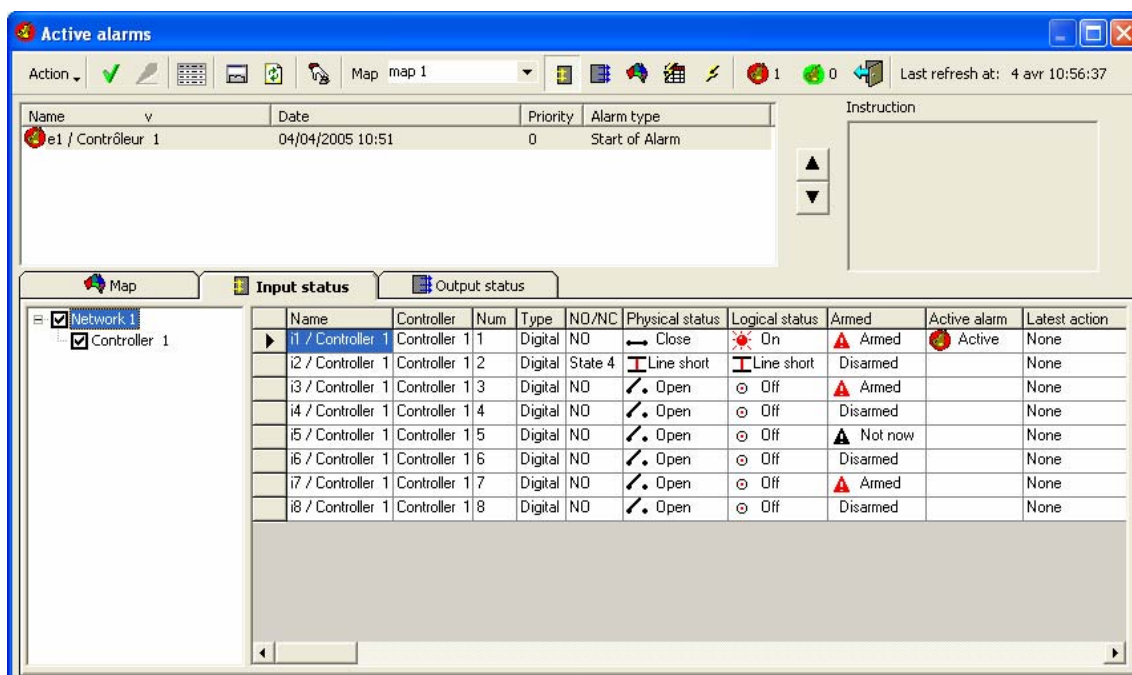
### **When an alarm is raised the system reacts**

- Log display: alarm displayed in red
- Journal: event is recorded
- Navigation bar: increase in the number of alarms raised
- “Active Alarms” screen: the icon connected to the alarm appears on the site map displayed
- “Active Alarms” screen: mention of the name of the input activated and the date of the event in the top table
- “Active Alarms” screen: instructions related to the alarm input are displayed in the “Instruction” window.

When several alarms are detected, the last alarm is displayed in the table at the top of the “Active Alarms” screen. By clicking on an alarm icon, the cursor automatically moves towards the corresponding row. The instructions displayed correspond to the alarm selected. Note that the order of the active alarm table can be manually sorted, by clicking on the column header. Such a sort cancel the default sort (by date), and therefore the last alarm may appear in the middle of the list.

### 4.4.3. Active Alarms - Input Status

This screen displays a dynamic activation status of the input. Before displaying the data, it may take about 15 seconds for checking all input status.



#### Table analysis

**Controllers list:** Select the required controllers. Inactive controllers are represented in grey

**Name:** Input name

**Controller:** Controller name that the input belongs to

**Num:** Input number in the controller.

**Type:** Mention if the input type is Digital, Digital 4 states or Analog.

**NO/NC:** Input normal status, i.e. normally open (NO), normally closed (NC) or State 1 to 4.

**Physical status:** Open, Close, Line short or Line cut. During reading time or communication problems with the controller, a '?' mark is displayed to show that the status is unknown.

**Logical status:** On, Off, Line short or Line cut (or '?' if the status is unknown).

**Armed:** The arm status switches between:

- **(Red icon) Armed:** The current time falls within the activation boundaries of the input weekly program ('green' periods').
- **(Black icon) Not now:** The current time falls outside the activation boundaries of the input weekly program ('red' periods).
- **Disarmed:** The input is not included within the Event Handling Program.

The system automatically goes from "Not now" to "Armed", and vice versa, according to time zones.

**Active alarm:** Coloured icons signal the alarm status (active, acknowledge and confirmed) in the table as well as in the tool bar

- **(Red icon) Active:** Active alarm
- **(Green icon) Acknowledge:** Acknowledge alarm
- **No icon:** Not in alarm or alarm confirmed

**Latest action:** Shows if the normal situation has not temporarily been affected manually or by the activation of an action, a process or a global reflex.

## Tips & Notes

### Manual action

Point the mouse on an input name, click on the right button and choose among the following functions:

- Acknowledge (when under alarm)
- Confirm (when under alarm)
- Open input properties
- Return to normal mode
- Input deactivation

### Sorting out information

The information in the table can be sorted out. Each column can serve as a sorting criterion. To organize information in an increasing order, click on the column header. To sort the information in a decreasing order, click again on the column header.

### Alarm prevention

To prevent the alarm apparition, resulting from input activation, choose one of the following methods:

- Delete the input from the input list (in "[Controller - Input](#)" screen).
- In the "[Event-Handling Program - Alarms](#)" screen, select **X** to exclude the input from the event-handling program.
- In the "[Event-Handling Program - Alarms](#)" screen, attribute the "WP Never" weekly program to the input.
- From the "[Active Alarms - Map](#)" screen or from the "Active Alarms - Input Status" screen, right click on the input and select 'Input deactivation'.

## Example

### How to set an alarm that would be active only at night:

The opening of a door must raise an alarm during the night (arming period) but not during the day (disarming period).

Perform as follows:

- In the "[Controller - Input](#)" screen, define the input to which the sensor that checks the door opening is connected.
- Define the arming period, in other words, the daily and weekly programs, which are activated at night and inactivated during the day (in the "[Parameter - Daily Program](#)" and "[Parameter - Weekly Program](#)" screen)
- In the "[Event-Handling - Alarms](#)" screen, select **V** to include the input in the event-handling program, and select the required Weekly program.
- If necessary, position the corresponding icon in a map.

During the night, the alarm will be activated if the door is opened. During the day, the input is disarmed by its weekly program and will not trigger an alarm.

**Note:** The "WP Always" weekly program permits to arm incessantly an input; the "WP Never" weekly program never arms an input. An input must be armed for its activation triggers an alarm in the "Active Alarms" screen.

#### 4.4.4. Active Alarms - Output Status

This table displays the output status, in real time. It is also accessible from the “[Manual Action - Relays control](#)” screen.

| Name              | Controller   | Num | Physical status | Time activation      | Latest action |
|-------------------|--------------|-----|-----------------|----------------------|---------------|
| r1 / Controller 1 | Controller 1 | 1   | Open            |                      | Constant ON   |
| r2 / Controller 1 | Controller 1 | 2   | Close           |                      | Constant OFF  |
| r3 / Controller 1 | Controller 1 | 3   | Close           |                      | None          |
| r4 / Controller 1 | Controller 1 | 4   | Open            | ON by weekly program | None          |

#### Table analysis

**Controllers list:** Select the required controllers. Inactive controllers are represented in grey

**Name:** Relay name

**Controller:** Controller name that the relay belongs to

**Num:** Output number in the controller.

**Physical status:** Open or Close. During reading time or communication problems with the controller, a ‘?’ mark is displayed to show that the status is unknown.

**Time activation:** This column shows if a Weekly Program has been attributed to the relay:

- **✓ ON by weekly program:** The relay is activated because a weekly program has been attributed and the current time falls within the activation boundaries of the weekly program (‘green’ periods). The relay is automatically activated according to time zones.
- **✗ OFF by weekly program:** The relay is deactivated because a weekly program has been attributed and the current time falls outside the activation boundaries of the weekly program (‘red periods’). The relay is automatically released according to time zones.
- **No text:** No weekly program has been attributed to the relay.

**Note:** The “WP Always” weekly program permits to trigger incessantly a relay while the “WP Never” weekly program ensues in a constant deactivation.

**Latest action:** Shows if the normal situation has not temporarily been affected manually or by the activation of an action, a process or a global reflex.

#### Tips & Notes

##### Manual action

Point the mouse on an output name, click on the right button and choose among the following functions:

- Open relays properties
- Return to normal mode: To cancel all actions described below.
- Deactivate relay continuously (Constant OFF): To close a door permanently for example
- Activate relay continuously (Constant ON): To open a door permanently for example
- Activate relay during: To switch on / off an indication light, during a defined delay for example. Specify the number of seconds (between 1 to 120 sec.).

##### Sorting out information

The information in the table can be sorted out. Each column can serve as a sorting criterion. To organize information in an increasing order, click on the column header. To sort the information in a decreasing order, click again on the column header.



## 5. “Modules” MENU

### 5.1. Time & Attendance Management Module

#### 5.1.1. Roll Call

This screen allows the time & attendance management. It facilitates the computation of employees' attendance, to provide the number of hours worked by employees.

It is a very basic calculation, which only takes into account the first and last access of a cardholder at pre-defined readers. The calculation can be restricted to specific periods.

#### Fields

**Start date:** Specify the date and hour of the beginning of the period

**End date:** Specify the date and hour of the end of the period

**Left window:** Select the reader(s) to take into account

**Right window:** Select the cardholders(s) to take into account

**Preview:** Preview the roll call report

| Roll call                                 |            |           |                    |              |
|---|------------|-----------|--------------------|--------------|
| From 12/04/2005 00:00 To 12/04/2005 23:59 |            |           |                    |              |
| <b>Johnson Greg</b>                       |            |           |                    |              |
| Date                                      | First pass | Last pass | Day total hours    |              |
| 12/04/2005                                | 14:25      | 14:26     | 00:01              |              |
|   |            |           | <b>Total hours</b> | <b>00:01</b> |
| <b>Smith John</b>                         |            |           |                    |              |
| Date                                      | First pass | Last pass | Day total hours    |              |
| 12/04/2005                                | 14:25      | 14:25     | 00:00              |              |
|   |            |           | <b>Total hours</b> |              |

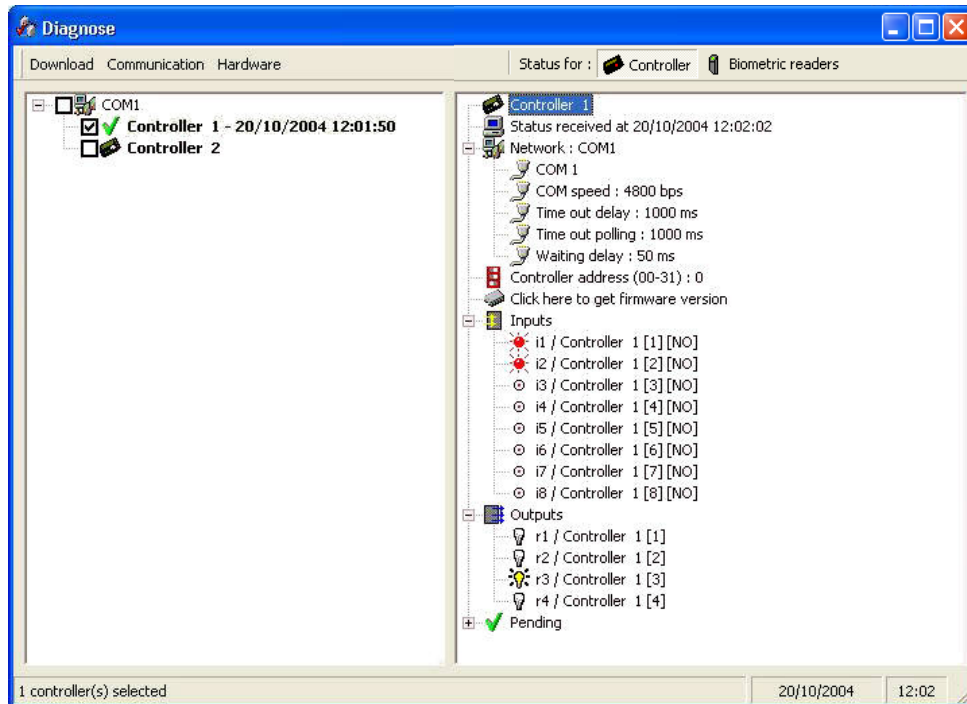
## 6. “Communication” MENU

### 6.1. Diagnose

The diagnose screen allows the visualization of the controllers status and the biometric readers status. This screen is made up of two windows:

- **Left window:** Controllers list / biometric readers list
- **Right window:** Information regarding the selected controller or biometric reader

Selecting a controller or biometric reader from the left window activates the right window where the details of the selected controller or biometric reader are displayed.



### Menu

**Download:** Menu of the available downloads for the selected controller or biometric reader

**Communication:** allows to check the communication with controllers:

- **Check communication (All)**
- **Check communication (selected):** Select the controller(s) to check (by clicking on the ☐ button next to the controller name)
- **Refresh every:** For automatic checking. Select the controller(s) to check and define the refresh delay in **Sec.**

**Hardware:** allows to check the inputs/outputs status of the controller displayed in the right window:

- **Refresh status:** Display before the selected controller details in the right window
- **Refresh every:** For automatic checking. Select the controller(s) to check and define the refresh delay in **Sec.**

**Status for:** Choose the information to display:

- **Controller:** Press this button to display the controllers status
- **Biometric readers:** Press this button to display the biometric readers status:  
From the 'Download' menu it may be possible to initialize one or several biometric readers by re-sending all the database templates after deleting all the fingerprint templates from the reader memory.

## Data displayed

**Left Window:** The controllers / biometric readers list, is sorted by their controller network.

Controller or biometric reader communication status is graphically represented as follows:

- **Grey:** if the controller or the biometric reader is not active, (the communication is not monitored by the system)
- **Bold:** if the controller or the biometric reader is active, (the communication is controlled by the system) in which case, by clicking on the controller or biometric reader name, **V** or **X** icon is displayed next to the name:
  - X:** absence of communication
  - V** (with date and hour): communication established; the controller or the biometric reader details are displayed in the right window

**Right window:** Details of the controller or the biometric reader selected in the left window

### **Controller or Biometric reader name**

**Status received at:** Date and hour of the event (the controller time when request was put in can differ from time of request if internal controller clock is late)

**Network type:** Network name, which the selected controller or biometric reader belongs to:

- Port and address of the network: COM, TCP or Modem
- Communication speed (in bauds)
- Time out delay (in milliseconds)
- Time out polling (in milliseconds)
- Waiting delay (in milliseconds)

### **Controller address (from 00 to 31) or Biometric reader address**

### Controllers specific data:

**Click here to get firmware version:** The date and the checksum of the firmware (Eprom or Flash) is displayed on the screen; this operation avoids checking physically, if needed.

**Inputs:** Inputs list with [input number] and [NO or NC definition]. An icon next to the input name specifies the input status (normal status, activated or undetermined) in real time.

**Outputs:** Outputs list with [relay number]. An icon next to the output name specifies the relay status (activated, deactivated or undetermined) in real time.

**Pending:** Selected controller commands list and their status. When downloading a non-connected controller, for instance, the information downloaded is signalled by the **V** symbol and the information pending by the **X** symbol.

### Biometric readers specific data:

**Unit type:** Biometric reader type (**1:N** means BioPass, **1:1** means BioProx or BioFlex).

**Memory Usage:** Appears in X / Y format where:

- X = Used templates
- Y = Maximum templates capacity.

**Pending:** Some actions related to the biometric readers may be not executed i.e. following to a temporary communication failure. These actions are stored in a buffer as pending commands and are executed later when communication is regained. These are the following actions:

- Delete the entire template of a cardholder
- Delete all templates of a given badge
- Delete all template of a biometric reader
- Delete a specific template
- Download all templates to a specific biometric reader
- Download cardholder templates to all the biometric readers
- Download a single template to all the biometric readers
- Replace an old badge with a new badge

When the **V** symbol is displayed near the title 'Pending', it means that all the fingerprint templates have been received well by the biometric reader.

## Tips & Notes

### Keyboard Shortcut

Use the "F8" function key at any time, to display the diagnose screen from the software main screen.

## 6.2. View / Clear Log

The log display is a temporary linear colour display that indicates events as they occur. Information to display in the log (and in the journal) can be customized in the "[Tools - Options - Messages](#)" screen. Through that screen an audit of records modifications can be recorded.

Note: Similar information can be recorded in the journal for later reference and printing. Although they appear similar, the contents of the log display and those of the journal are not 100% identical. For example, the user login appears in the journal but not in the log display, by default.

### Messages

By default different colours indicate the type of information available:

**Burgundy:** For signalling unknown badges (not recognized by the system), non-allocated badge (recognized by the system but not allocated) or system alarms, such as weak battery, power up after failure, memory deleted, etc.

**Red:** For signalling the start and end of input activation

**Green:** For signalling an access authorization and a normal communication status (OK)

**Black:** For signalling an access denied and its denied reason

**Grey:** For signalling system commands, provided for informational purposes. They are not displayed by default.

## Tips & Notes

### Customization of the Log Display

The “[Tools - Options - Journal / log screen](#)” screen displays different customization: view/hide log windows at start-up, separate log windows for alarms and access, define a personal log windows size, show system commands for information.

## Rich Log

Rich log allows seeing icons linked to a context menu. It is available by choosing the ‘Rich log’ option on the “[Tools - Options - Journal / log screen](#)” screen.

- **Context menu:** By clicking right on some log events, here are the available commands:
  - Open cardholder screen:** Open the associated [cardholder screen](#).
  - Open reader screen:** Open the associated [reader screen](#).
  - Open input screen:** Open the associated [input screen](#).
  - Open controller screen:** Open the associated [controller screen](#).

## 6.3. Display Photo

This screen displays the cardholder’s picture which asks for access at a specific reader. It allows to compare the appearance of the person presenting his badge at a reader to the photograph associated to the badge and stored in the system.

Note: The screen size can be adjusted.

### Fields

**From readers:** Select the reader(s) or the access group(s) for which the identification check is requested

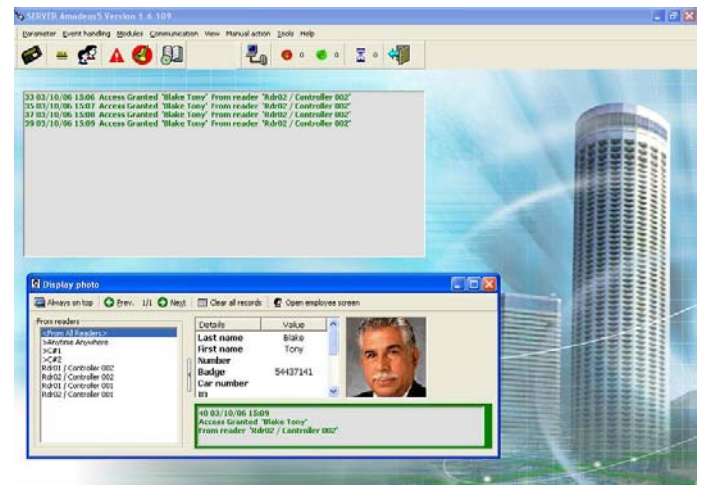
**Always on top:** Check this box to show this screen even if other screens are opened

**Open employee screen:** Click on this button to open the [current employee](#) screen

**Clear all records:** Clear the displayed employees list

**Buttons [◀] & [▶]:** Click on these buttons to skip from one record to the next

**Number/Number:** Number of the current employee on the total number of displayed employees



## 7. “Tools” MENU

### 7.1. Report wizard

ProNet system incorporates a powerful report wizard for generation, modification and update of personalized reports. Reports are compiled from the journal or from any other information of the database (parameters, events or modules). They are generated in the language of the application. They can be displayed, printed or exported.

This screen allows the creation of a standard journal report based on customized queries.

## Fields

**Select the report data to display:**

- **From Current Journal** (by default)
- **From another journal:** Select the journal by using the [...] button (with "Access" database ONLY)

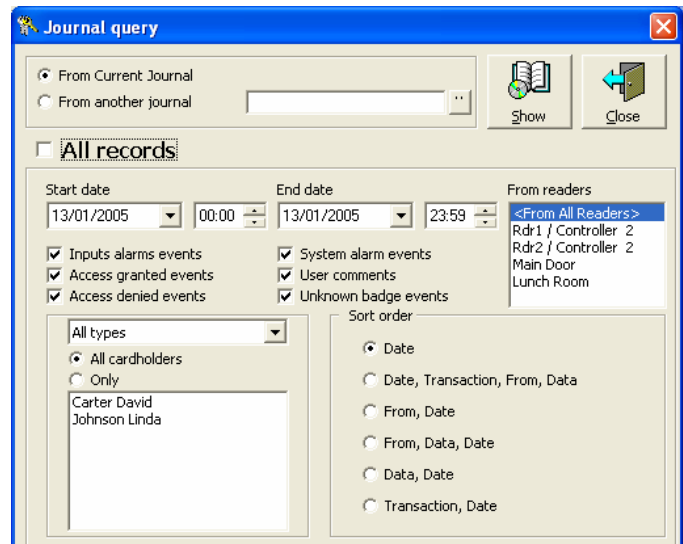
**All records:** Check this box to display all the information available in the system; the bottom part of the screen is shaded grey. If this option is not checked, the bottom part of the screen is activated to allow the selection of the data filtering criteria.

**Filtering and Sorting out data:** Select the data filtering criteria from the journal

- **According to date:** Select the date and hour of the start and the date and hour of the end.
- **According to reader:** Select the required reader(s).
- **According to events:** Choose the events to keep: Inputs alarms, Access granted, Access denied, System alarm, User comments, Unknown badge.
- **According to cardholders:** Select the required cardholder(s).
- **Sort order:** Select the desired display order of the data.

**Show:** Click to display the report data.

**Close:** Click to close the report wizard and go back to the main screen.



### 7.1.1.2. Report wizard - Preview

This screen allows the preview of an existing report before printing and/or exporting.

**Export:** Click to export the selected report in the following RTF - Rich Text Format

- PDF - Portable Document Format
- HTML - Hyper Text Markup Language
- XLS - Microsoft Excel
- TIF - Tagged Image Format
- TEXT

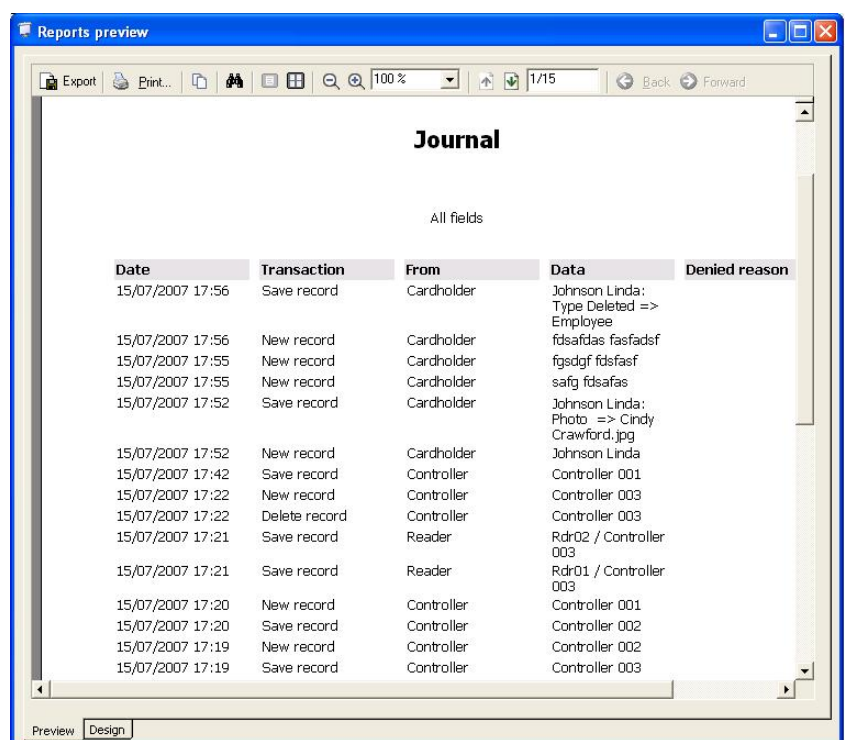
**Print:** Click to print after having specified printing parameters.

**Copy this page in the clipboard:**  
Click to copy the current page only

**Find:** Click to search for a specific word in the selected report.

**Single Page, Multiple Page, Zoom Out, Zoom In, Zoom:** Click to adjust the report preview.

**Previous Page, Next Page, Page:**  
Click to navigate in the report.



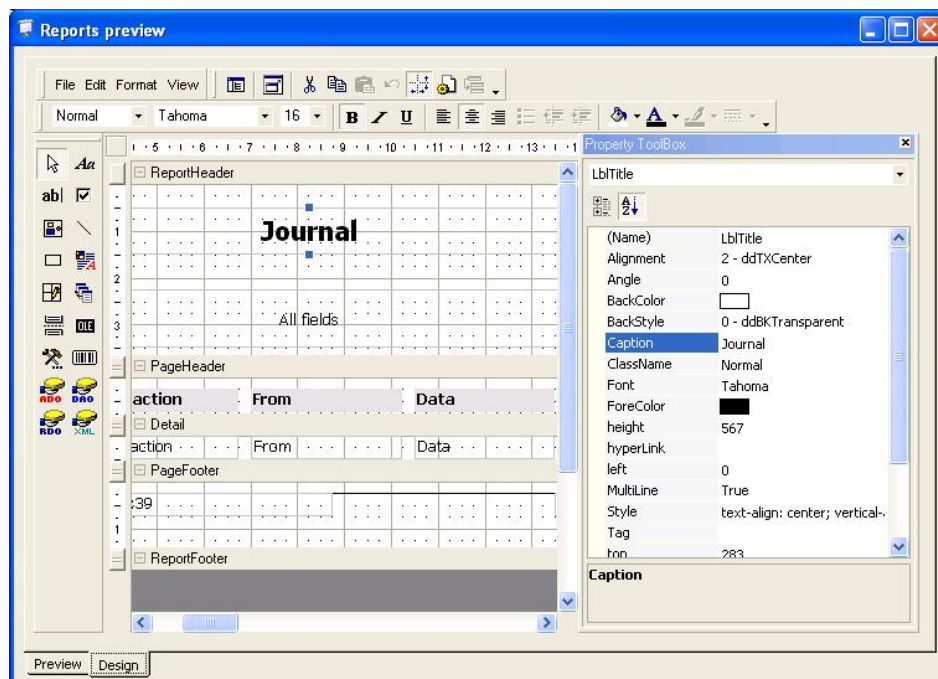
| Date             | Transaction   | From       | Data   | Denied reason |
|------------------|---------------|------------|--|---------------|
| 15/07/2007 17:56 | Save record   | Cardholder | Johnson Linda:<br>Type Deleted =><br>Employee    |               |
| 15/07/2007 17:56 | New record    | Cardholder | fdsafdas fasdfasf                                |               |
| 15/07/2007 17:55 | New record    | Cardholder | fgsdgf fdfsasf                                   |               |
| 15/07/2007 17:55 | New record    | Cardholder | safg fdfsafas                                    |               |
| 15/07/2007 17:52 | Save record   | Cardholder | Johnson Linda:<br>Photo => Cindy<br>Crawford.jpg |               |
| 15/07/2007 17:52 | New record    | Cardholder | Johnson Linda                                    |               |
| 15/07/2007 17:42 | Save record   | Controller | Controller 001                                   |               |
| 15/07/2007 17:22 | New record    | Controller | Controller 003                                   |               |
| 15/07/2007 17:22 | Delete record | Controller | Controller 003                                   |               |
| 15/07/2007 17:21 | Save record   | Reader     | Rdr02 / Controller<br>003                        |               |
| 15/07/2007 17:21 | Save record   | Reader     | Rdr01 / Controller<br>003                        |               |
| 15/07/2007 17:20 | New record    | Controller | Controller 001                                   |               |
| 15/07/2007 17:20 | Save record   | Controller | Controller 002                                   |               |
| 15/07/2007 17:19 | New record    | Controller | Controller 002                                   |               |
| 15/07/2007 17:19 | Save record   | Controller | Controller 003                                   |               |



| Date               | Transaction   | From       | Data                  |
|--------------------|---------------|------------|-----------------------|
| 15/07/2007 17:56:2 | Save record   | Cardholder | Johnson Linda: Type   |
| 15/07/2007 17:56:1 | New record    | Cardholder | fdsafdas fasfadsf     |
| 15/07/2007 17:55:5 | New record    | Cardholder | fgsdgf fdsfadsf       |
| 15/07/2007 17:55:3 | New record    | Cardholder | safig fdsafas         |
| 15/07/2007 17:54:0 | Save record   | Cardholder | Johnson Linda: Type   |
| 15/07/2007 17:52:5 | Save record   | Cardholder | Johnson Linda: Phot   |
| 15/07/2007 17:52:4 | New record    | Cardholder | Johnson Linda         |
| 15/07/2007 17:51:3 | Save record   | Cardholder | Johnson Linda: Type   |
| 15/07/2007 17:51:1 | Save record   | Cardholder | Albert Fisher: Numbe  |
| 15/07/2007 17:50:4 | Save record   | Cardholder | Albert Fisher: Photo  |
| 15/07/2007 17:42:0 | Save record   | Controller | Controller 001        |
| 15/07/2007 17:22:2 | New record    | Controller | Controller 003        |
| 15/07/2007 17:22:1 | Delete record | Controller | Controller 003        |
| 15/07/2007 17:21:5 | Save record   | Reader     | Rdr02 / Controller 0C |
| 15/07/2007 17:21:4 | Save record   | Reader     | Rdr01 / Controller 0C |
| 15/07/2007 17:20:1 | New record    | Controller | Controller 001        |
| 15/07/2007 17:20:0 | Save record   | Controller | Controller 002        |
| 15/07/2007 17:19:4 | New record    | Controller | Controller 002        |
| 15/07/2007 17:19:1 | Save record   | Controller | Controller 003        |

### 7.1.1.3. Report wizard - Design

This screen is reserved for confirmed users only. It allows the design of an existing report. Clicking on the '[Preview](#)' tab displays the preview of the report; it is useful to check the new modifications in real time.



## Operating Mode

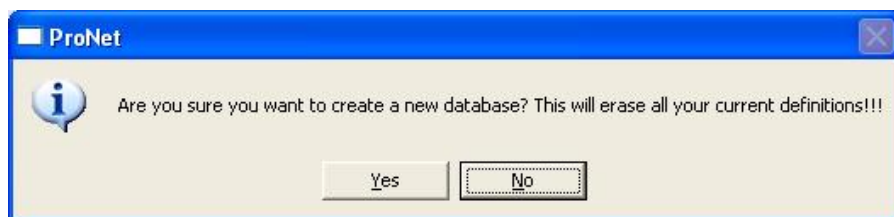
The Design tab is based on a professional tool of Active Report ®. In this manual we will not cover the large variety of options but we only give some basic instruction and tips:

- **Moving selected fields:** Select an existing field and drag and drop to the required position in the window.
- **Lengthen or shorten the space allocated to a field:** Select an existing field and drag the blue squares around the field to resize it.
- **Delete a field:** Select an existing field and delete it.
- **Change the text in a label/text box:** Select the field and edit the text on the 'Property ToolBox' window, in 'Caption' (for a label) or 'Text' (for a text box). Don't change 'Name'.
- **Change the font:** Select an existing field and change the font on the 'Property ToolBox' window, in the 'Font' field.
- **Add a new field or a picture:** Select the field type from the toolbar on the left and drop it in the layout. If it is a picture field, go to the "Picture" field of the 'Property ToolBox', click on the [...] button and browse your PC for any graphic file.
- **Change the Report Header background:** Select the Report Header window and change in the 'Property ToolBox' window, the "BackColor" field and set the "BackStyle" field to 1.
- **Save all changes:** Select the 'File/Save' menu and save the report on the 'Reports' folder under the application folder with RPX format.

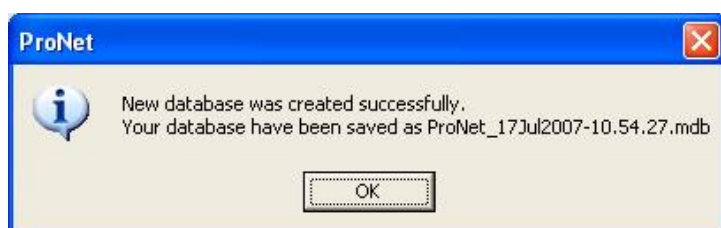
## 7.2. Create New Database

The ProNet application allows the storage of several databases. The application installer has thus a constant access to all sites databases. This command permits to create a new clean database, which becomes the active database.

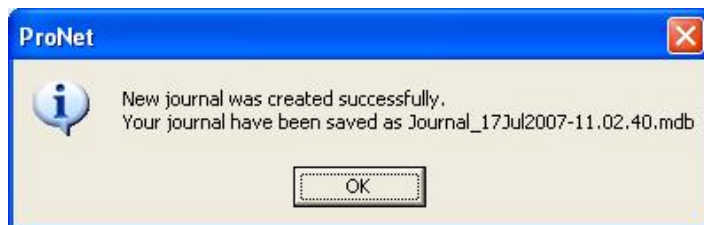
A warning message is displayed before applying the request in case of wrong action.



Information from the current database is saved. The system displays in a message (see opposite) the name of the saved file.



A database creation leads to create a new journal. The system displays in a message (see opposite) the filename, which contains the former journal.



The extension of the file is 'mdb' (Access database only). By default, the files are saved in the directory: "C:\ProgramFiles\ProNet5\Backup".

The default destination can be modified in the "[Tools - Options - Files Location](#)" screen.

### 7.3. Save Database

This command permits to save the database. The size of the ProNet database cannot exceed 70Mb for good operating condition. Once a month, it is therefore advisable to clean the system of unnecessary data.

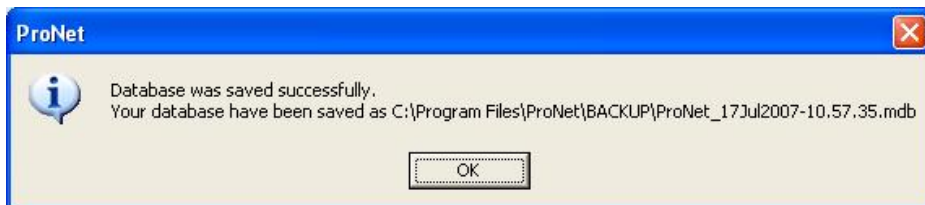
By selecting this command, the system opens a saving window with the Windows functions. By default, the system names the saving file with the current time and date automatically, but the name can be modified. To overwrite a database, select it from the displayed list and confirm or cancel the operation.

The system displays in a message (see opposite) the name of the saved file.

By default, the files are saved in the directory:

“C:\ProgramFiles\ProNet5\Backup”.

The default destination can be modified in the “[Tools - Options - Files Location](#)” screen.

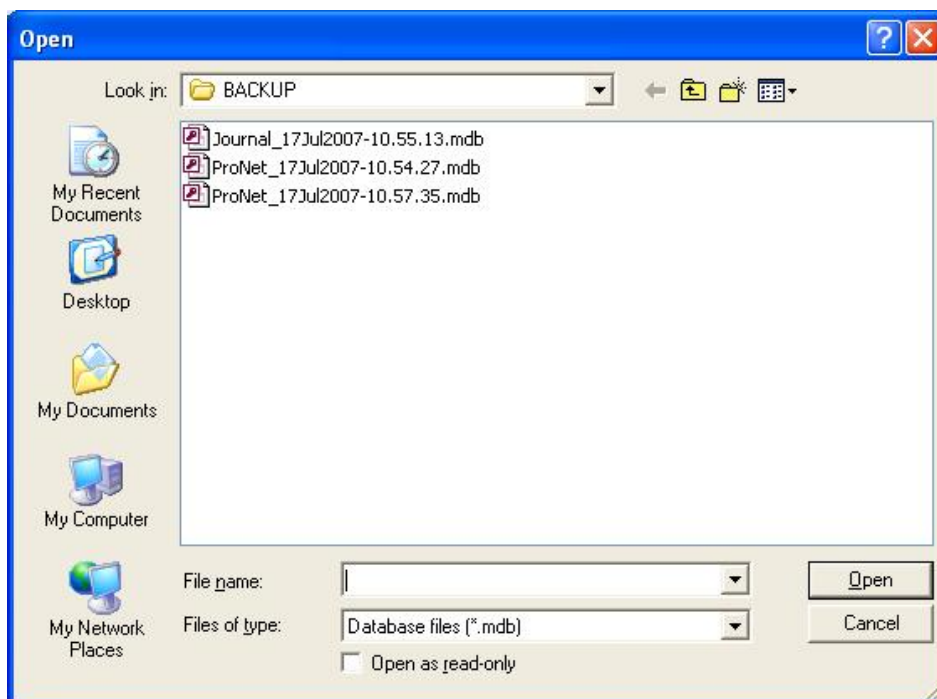


### 7.4. Restore Database

This command permits to restore a saved database. By selecting this command, the system opens a loading window with the Windows functions.

If using the Multi-company Module, this option will be available for super-users only (See the “[Multi Company Module](#)” chapter for further reference).

To restore a database, select it from the list displayed and confirm or cancel the operation. If the operation is confirmed (and if the chosen file contains a valid ProNet database), then the system saves the current database and replaces it with the new one.



#### Fields

**Look in:** Select the folder where is located the required database. By default, the selected folder is: “C:\ProgramFiles\ProNet5\Backup”. This default destination can be changed in the “[Tools - Options - Files Location](#)” screen

**File name:** Enter the filename containing the database

**Files of type:** Select the file type

- Database files (\*.mdb): Default extension for Access database
- Database files (\*.bak): Default extension for SQL database
- All files (\*.\*) : Ability to open a database created by other applications

**Open as read-only:** Check this box if the database is loaded for consultation only.

Once the restoring is done, the system displays a message (see opposite), with the filename of the former database.

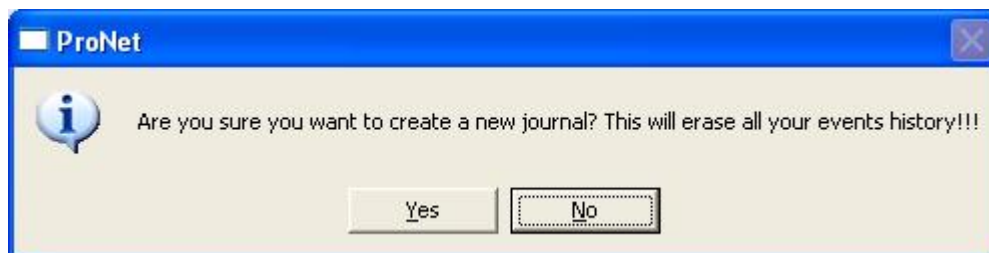


## 7.5. Create New Journal

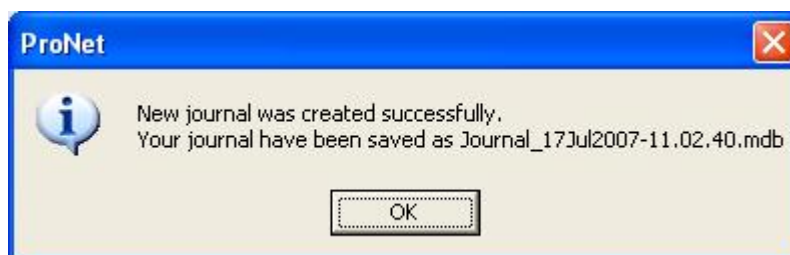
A journal is a database of all the events that have occurred in the system. The ProNet application allows the storage of several event journals and permits to consult them easily.

For good operating condition, it is recommended not to let the journal grow more than 150Mb. When the journal reaches this size, it is time to use this command for creating a new journal. This command automatically saves the current journal in a back-up file and creates a new clean one. Then, this clean journal becomes the current journal. ***This command is NOT available with SQL database.***

A warning message is displayed before applying the request in case of wrong action.



The system displays in a message (see below) the filename, which contains the former journal. The system automatically names the saving files with the current time and date.



The extension of the file is 'mdb' (Access database only). By default, the files are saved in the directory: "C:\ProgramFiles\ProNet5\Backup".

The default destination can be modified in the "[Tools - Options - Files Location](#)" screen.

### Tips & Notes

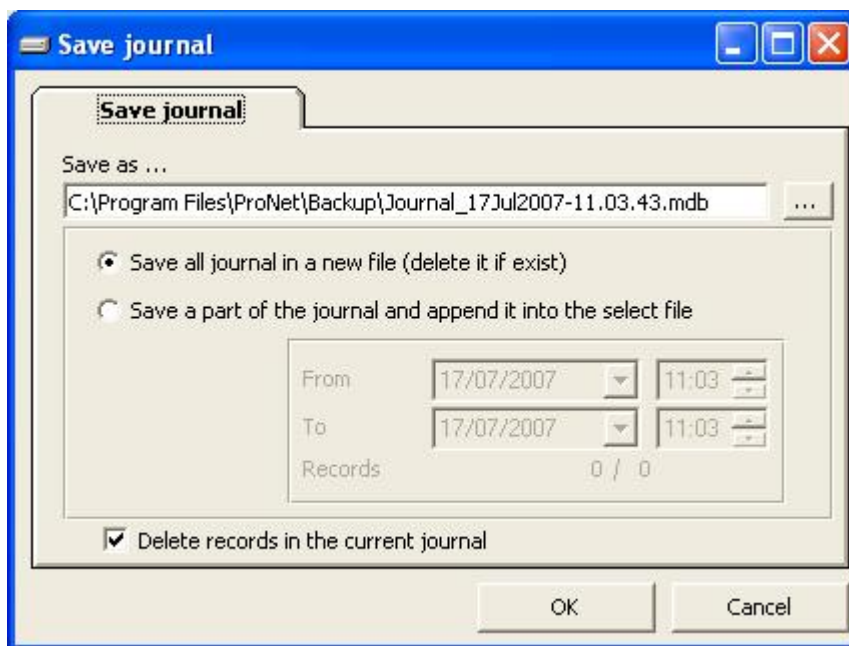
#### **Automatic Journal creation**

It can be useful to create a global reflex that will renew the journal on an automatic and a regular basis, each 2 months for example (For more details, see the "[Event handling - Action](#)" and "[Event handling - Global Reflex](#)" screens).

## 7.6. Save Journal

This command permits to save regularly the entire or a part of the journal. For good operating condition, it is recommended not to let the journal grow more than 150Mb.

By selecting this command, the system opens the following screen. By default, the system names the saving file with the current time and date automatically, but the name can be modified.



### Fields

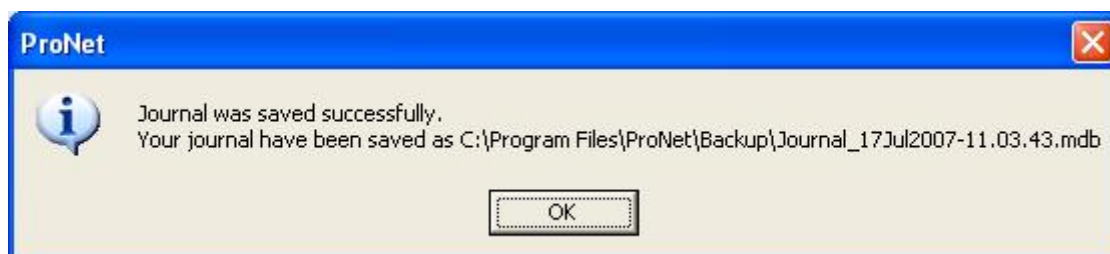
**Save as:** Accept or modify the name suggested or select an existing filename using the [...] button.

**Choose one of the following options:**

- **Save all journal in as a new file (delete if exists)** (default option)
- **Save a part of the journal and append it into the selected file**
  - From:** Specify start date and hour of journal
  - To:** Specify end date and hour of journal
  - Records:** Number of selected records and total records number

**Delete records in the current journal:** Default option

Once the saving is done, the system displays in a message (see below) the name of the saved file.



By default, the files are saved in the following directory:

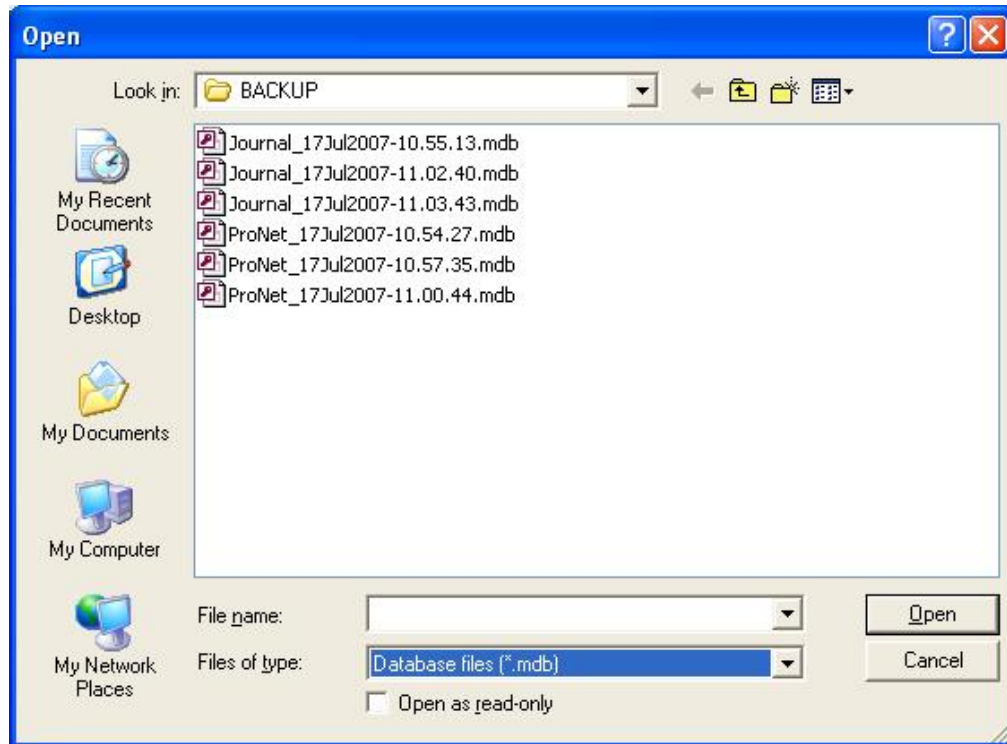
"C:\ProgramFiles\ProNet5\Backup". The default destination can be modified in the "[Tools - Options - Files Location](#)" screen.



## 7.7. Restore Journal

This command permits to restore the data of a saved journal. By selecting this command, the system opens a loading window with the Windows functions.

To restore a journal, select it from the list displayed and confirm or cancel the operation. If the operation is confirmed (and if the chosen file contains a valid ProNet journal), then the system saves the current journal and replaces it with the new one.



### Fields

**Look in:** Select the folder where is located the required journal. By default, the selected folder is: "C:\ProgramFiles\ProNet5\Backup". This default destination can be changed in the "[Tools - Options - Files Location](#)" screen

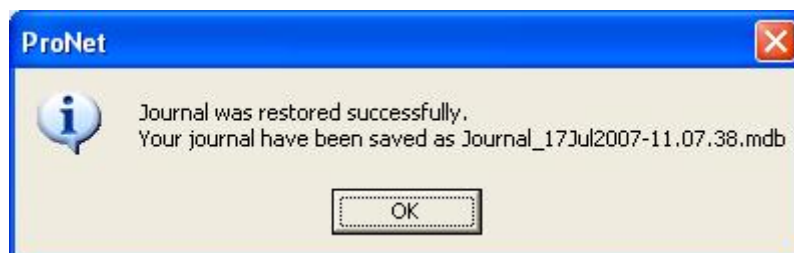
**File name:** Enter the filename of the journal

**Files of type:** Select the file type

- Database files (\*.mdb): Default extension for Access database
- Database files (\*.jrn): Default extension for SQL database
- All files (\*.\*) : Ability to open a journal created by other applications

**Open as read-only:** Check this box if the journal is loaded for consultation only.

Once the restoring is done, the system displays a message (see below), with the filename of the former journal.





## 7.8. Create a group of badges

This menu allows creating or removing a group of badges in a single command.

It is accessible via the “[Parameter - Badge](#)” or “Tools - Create a group of badges” menu.

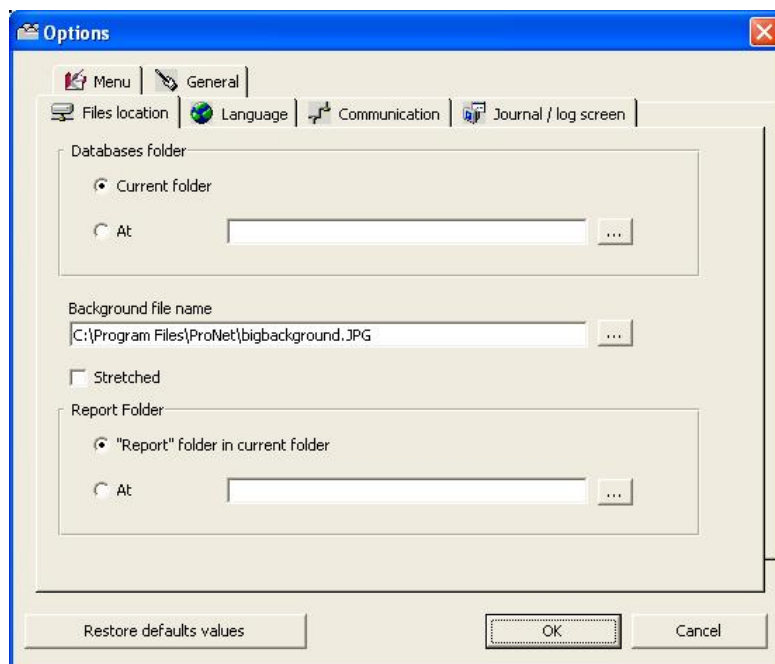
Refer to the “[Group of Badges](#)” paragraph for further information.



## 7.9. Options

This screen defines the different using parameters of ProNet. It is divided into six tabs:

- [Files location](#)
- [Language](#)
- [Communication](#)
- [Journal / log screen](#)
- [General](#)
- [Menu](#)



At the bottom of each tab, three buttons are always displayed:

- **Restore default values:** Click for recovering the original configuration.
- **OK:** Click for saving the new changes and back to the main screen.
- **Cancel:** Click for cancelling the new changes and back to the main screen.

### 7.9.1. Files Location

This tab defines the folder location of the database files and the background picture of the main screen.

#### Fields

**Databases folder:** Choose the database files location:

**Current folder:** The software folder, by default.

**At:** Indicate the desired databases directory by using the [...] button.

**Background filename:** Select the desired file by using the [...] button.

**Stretched:** Check this box to stretch the selected background picture on the entire screen.

**Report folder:** Choose the reports files location:

**“Report” folder in current folder:** The software folder, by default.

**At:** Indicate the desired directory by using the [...] button.

### 7.9.2. Language

ProNet supports many languages. Specify the requested language and confirm your choice. Screens and functions are translated instantaneously, with no need to reboot the application.

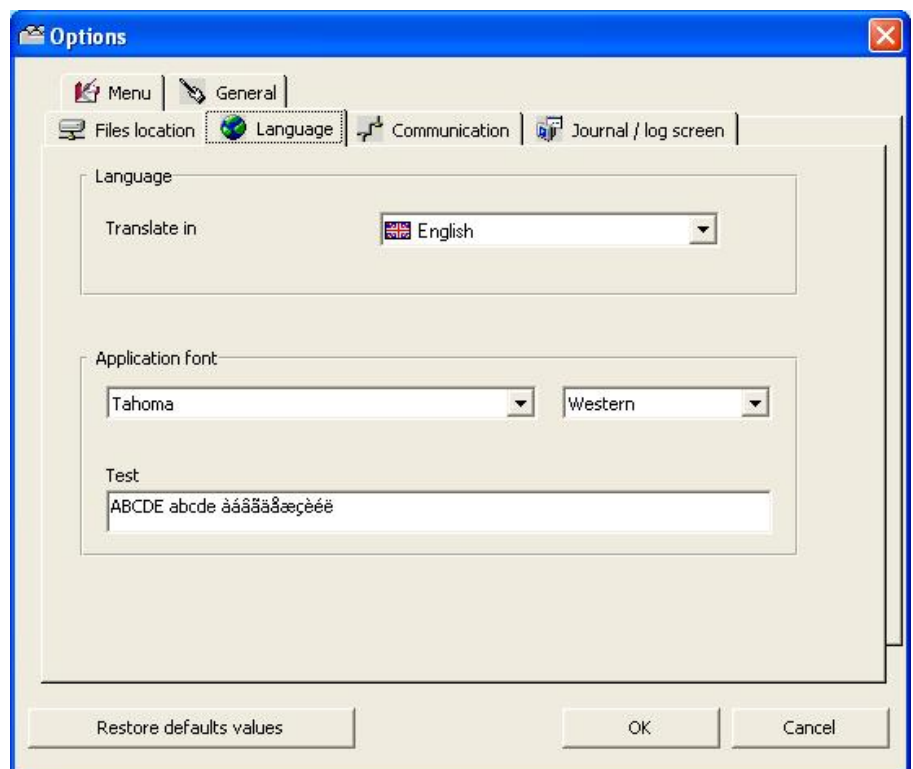
#### Fields

**Translate in:** Select from the list the required language. All screens and menus will be translated.

**Application font:** Select the desired font. It concerns all menus and screens.

**Font according to the language:** Select the font type according to the alphabet used (Chinese, Western, etc.)

**Test:** Example that serves for checking how the selected font is displayed.



### 7.9.3. Communication

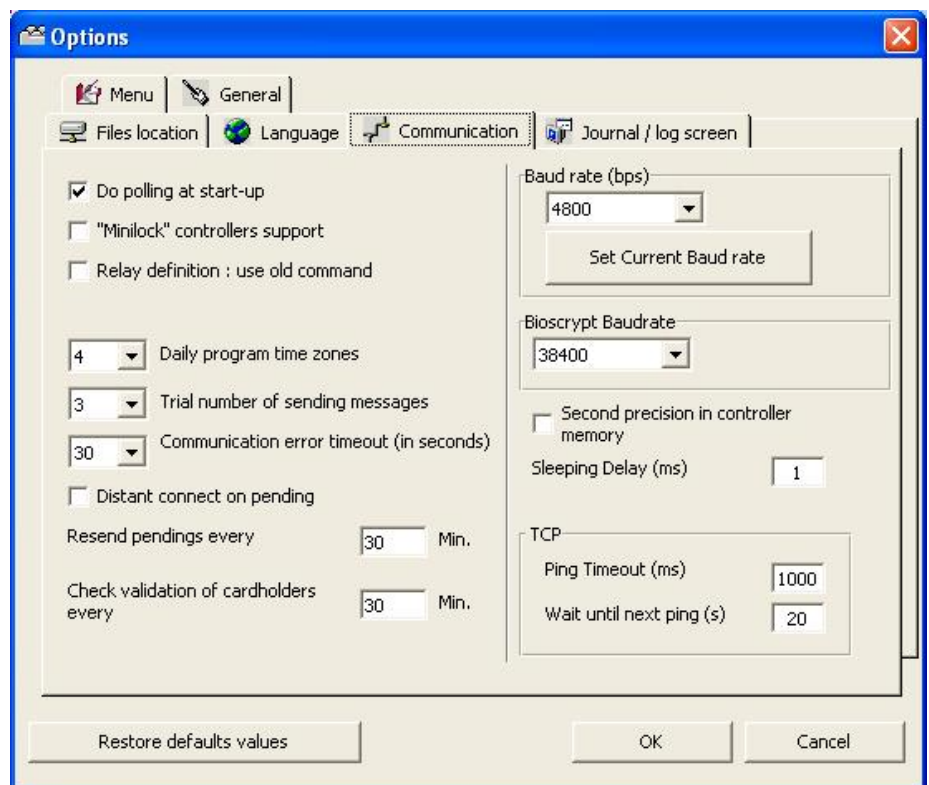
Default communication parameters are defined in this tab. ***This tab will NOT be displayed if the application runs as a Workstation.***

#### Fields

**Do polling at start-up:** Check this box to execute polling when loading the application. By default, this option manually stopped by choosing the [“Communication - Stop Polling”](#) menu or by pressing on “SHIFT” and “F8” keys simultaneously.

**“Minilock” controllers support:** Check if this specific controller is used.

**Daily program time zones:** Choose among 2 (by default) or 4 for modifying the number of daily programs (consult also the [“Daily Program”](#) chapter).



**Trial number of sending messages:** Choose between 1 to 10 (3 by default) for modifying the number of times a command will be sent to the controller in case of absence of communication between PC and controller (see the [“Time out delay”](#) paragraph in the “Controller Network” chapter). If the command is still not received, this command joins the “Pending” commands and the PC will try to send it with the other pending commands once the communication established (see the “Resend pending” option below).

**Communication error time out (in seconds):** Choose between 1 to 300 (30 by default) for modifying the delay beyond which the computer will signal a communication problem, in case of absence of communication between PC and controller (see the [“Time out polling”](#) paragraph in the “Controller Network” chapter).

**Distant connect on pending:** Check this box for performing modem dial-up when pending commands are sent (see the [‘Updating dial up controllers’](#) section).

**Resend pending every X Min.:** Enter a value (30 by default). Pending commands are commands that a controller has not received (usually in case of a communication problem) and will be sent again, by default, every 30 minutes (default value) till the communication recovering.

**Check validation of cardholders every X Min.:** Enter a value (30 by default). Every 30 minutes (default value), the program checks if new cardholders need validating or invalidating, in which case the corresponding cardholders definitions are sent to the controllers. The default frequency of this checking (30 minutes) may be modified here.

**Baud rate (bps):** Select from the list the controller baud rate. This rate is the same for all the controllers.

**Set current Baud rate:** Click on this button for sending immediately the selected baud rate to all the controllers.

**Bioscript Baud rate:** Select from the list the biometric reader baud rate. This rate is the same for all the biometric readers.

**Second precision in controller memory:** Check this box for setting the controllers to send the exact seconds value of an event. A one-time init of all controllers is required after this setting is being changed.

**Sleeping Delay (ms):** Waiting delay between two consecutive commands that PC sends to the controllers.

**TCP:**

**Ping Timeout (ms):** Maximum delay that PC gives to the TCP/RS485 converter to answer after a Ping (question from the PC to the converter).

**Wait until next ping (s):** When the TCP/RS485 converter does not answer after the first ping, the PC awaits this delay before pinging it again.

#### 7.9.4. Journal / Log Screen

This tab allows the log window customizing.

The log display is a temporary linear colour display that indicates events as they occur in the system. The events are displayed as they take place (consult also the [“View / Clear Log”](#) chapter).

Changes take effect instantaneously, no need to reboot the application.

##### Fields

**View log window at start-up:** Select ‘Yes’ or ‘No’ as required.

**Separated logs for alarm and access:** Select ‘Yes’ in order to divide the log window in two parts: one with the access and system messages, and the other with the alarm messages. By default, a single log shows access, alarms and system messages.

**Log window size:** To modify the size of the log window, choose among the following options:

**Standard window:** By default (Height: 3735, Width: 9015, Top: 480, Left: 240).

**Maximized window:** Depends on the screen definition.

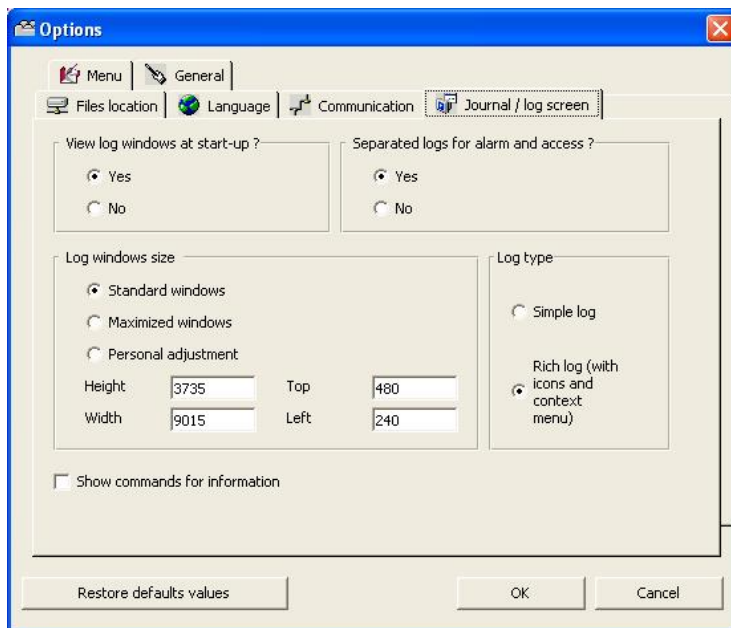
**Personal adjustment:** Specify the required values for height, width and the window positioning at the top and at the left.

**Log type:**

**Simple log:** By default

**Rich log (with icons and context menu):** Enables using a right-click menu with some shortcut option at the main log. Such as getting historical video records from the events rows of the log (see details at the [“Rich Log”](#) paragraph).

**Show commands for information:** Check this box for showing the system commands in the log display. This option is purposed for application developers mostly; this is the reason why it is not selected by default.



### 7.9.5. Menu

This tab gives the possibility to choose which are event types to save in the journal and which are event types to display on the log. In this last case, it is possible to modify the messages colour of the log (see also the [“View / Clear Log”](#) chapter).

Changes take effect instantaneously, no need to reboot the application.

By default, all event types are saved in the journal and most of them are viewable on the log window.

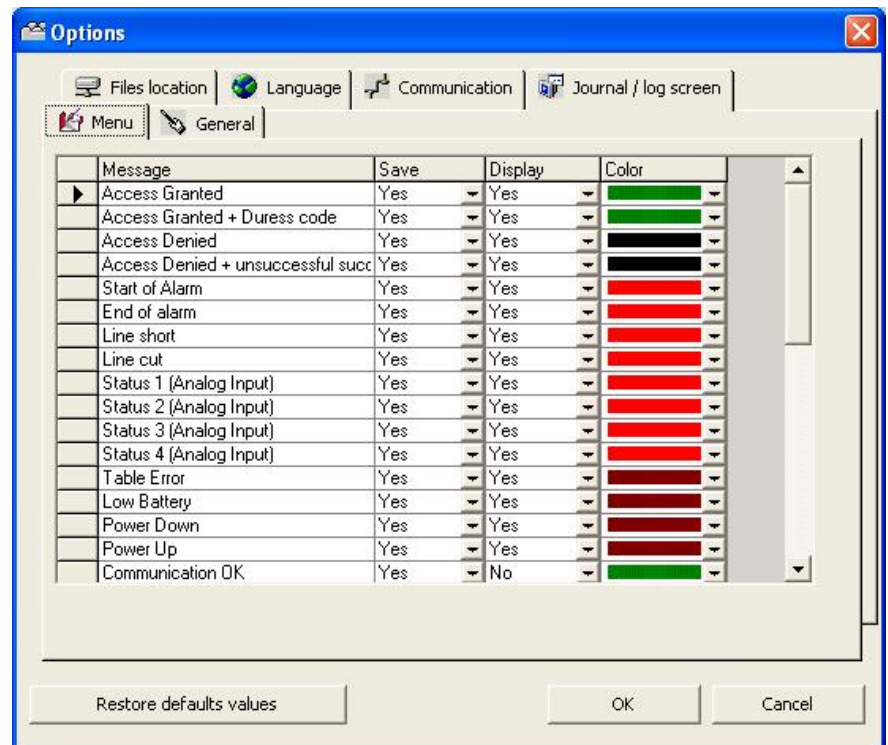
#### Fields

**Message:** Name of the event type.

**Save:** Select ‘Yes’ for saving this event type in the journal.

**Display:** Select ‘Yes’ for displaying this event type on the log.

**Colour:** Select the message colour for log display; consult the [“View / Clear Log”](#) chapter for the default colours of the messages.



#### Tips & Notes

#### Audit of the Database changes

To perform an audit of the database modifications entered by different users, save (and eventually display) the following event types:

- New Record,
- Save Record,
- Delete Record.

Then, for each record modification, the following information is accessible:

- What: Record creating, changing or deleting
- Which Screen: Name of the screen in which the database modification has been done
- Which Record: Name of the record on which the modification has been done
- Details of the modification (for badges and cardholders): Old value => New value
- Who: Name of the user which has modified the record



### 7.9.6. General

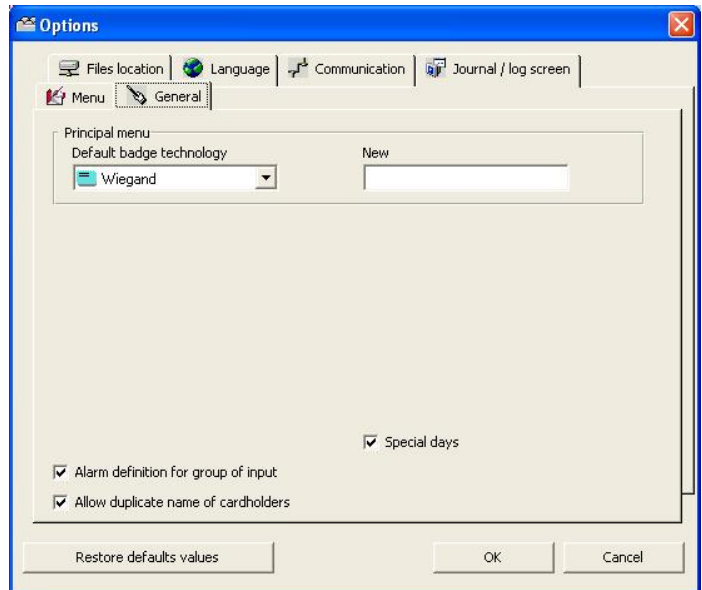
This screen defines default values for some parameters like badge technology, badge code, main screen toolbar and automatic log off.

#### Fields

##### Badge:

**Default badge technology:** Each site works generally with a main badge technology; the system creates new badges using the technology, which is selected here, without having to specify the technology used at each badge creating.

**Default Badge Code:** Type a beginning card code common to all badges, if needed; this is useful when the site code is not written on the badges.



**Alarm definition for group of input:** Check this box for displaying the fields related to input groups in the "[Input - Alarm status](#)" screen and defining an input group weekly program in the "[Event-Handling Program – Alarms](#)" screen.

**Allow duplicate name of cardholders:** Check this box for creating cardholders with the same last and first name. In this case, it is necessary to enter a unique number per person in the "Number" field of the "[All cardholders](#)" screen.

**Special days:** Check this box for adding two supplementary daily programs (S1-S2). See more details at the "[Weekly Program](#)" chapter.

Note: This feature requires a supporting firmware, please check with your vendor.